Y4. Sci 2:97/110

IMPACT OF NATIONAL SECURITY CONSIDERATIONS ON SCIENCE AND TECHNOLOGY

Y4. Sci 2:97/110

ORIGINAL
COMPLETED

HEARING

BEFORE THE

SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY

AND THE

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

NINETY-SEVENTH CONGRESS

SECOND SESSION

MARCH 29, 1982

[No. 110]

Printed for the use of the
Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE

97-341 O WASHINGTON : 1982

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MARILYN LLOYD BOUQUARD, Tennessee
JAMES J. BLANCHARD, Michigan
TIMOTHY E. WIRTH, Colorado*
DOUG WALGREN, Pennsylvania
RONNIE G. FLIPPO, Alabama
DAN GLICKMAN, Kansas
ALBERT GORE, JR., Tennessee
ROBERT A. YOUNG, Missouri
RICHARD C. WHITE, Texas
HAROLD L. VOLKMER, Missouri
HOWARD WOLPE, Michigan
BILL NELSON, Florida
STANLEY N. LUNDINE, New York
ALLEN E. ERTEL, Pennsylvania
BOB SHAMANSKY, Ohio
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
MERVYN M. DYMALLY, California

LARRY WINN, JR., Kansas
BARRY M. GOLDWATER, JR., California
HAMILTON FISH, JR., New York
MANUEL LUJAN, New Mexico
HAROLD C. HOLLENBECK, New Jersey
ROBERT S. WALKER, Pennsylvania
EDWIN B. FORSYTHE, New Jersey
WILLIAM CARNEY, New York
MARGARET M. HECKLER, Massachusetts
F. JAMES SENSENBRENNER, JR., Wisconsin
VIN WEBER, Minnesota
JUDD GREGG, New Hampshire
RAYMOND J. McGRATH, New York
JOE SKEEN, New Mexico
CLAUDINE SCHNEIDER, Rhode Island
JIM DUNN, Michigan
BILL LOWERY, California

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
REGINA A. DAVIS, *Administrator*
GERALD E. JENKS, *Minority Staff Director*

SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY

DOUG WALGREN, Pennsylvania, *Chairman*

GEORGE E. BROWN, JR., California
BOB SHAMANSKY, Ohio
MERVYN M. DYMALLY, California
STANLEY N. LUNDINE, New York
ALLEN E. ERTEL, Pennsylvania
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma

MARGARET M. HECKLER, Massachusetts
VIN WEBER, Minnesota
JUDD GREGG, New Hampshire
JOE SKEEN, New Mexico
EDWIN B. FORSYTHE, New Jersey

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

ALBERT GORE, JR., Tennessee, *Chairman*

BOB SHAMANSKY, Ohio
HAROLD L. VOLKMER, Missouri

ROBERT S. WALKER, Pennsylvania
MANUEL LUJAN, JR., New Mexico

*On assignment to Budget Committee for 97th Congress.

CONTENTS

WITNESSES

March 29, 1982: Page

Adm. Bobby R. Inman, Deputy Director, Central Intelligence Agency; Hon. Lawrence J. Brady, Assistant Secretary, International Trade Administration, Department of Commerce; and George P. Millburn, Acting Deputy Under Secretary for Research and Engineering, Department of Defense, accompanied by Dr. Leo Young, Director of Research and Technical Information, and Dr. Frank Kapper, Director of Military Technology, Office of International Programs and Technology 4

Dr. Frank Press, President, National Academy of Sciences; and Dr. Robert M. Rosenzweig, Vice President for Public Affairs, Stanford University 62

Dr. Robert Corell, Director, Sea Grant and Marine Programs, University of New Hampshire; Dr. Edward Gerjuoy, Professor of Physics, University of Pittsburgh; and Dr. John McLucas, President, World Systems Division, Comsat 111

APPENDICES

Additional material submitted for the record:

Soviet acquisition of Western technology 159

Executive branch comments on testimony of public witnesses 175

Papers presented at symposium on "Striking a Balance: Scientific Freedom and National Security," 1982 annual meeting of the American Association for the Advancement of Science, Washington, D.C. 178

Letters from the Chamber of Commerce of the United States of America to the U.S. Trade Representative 264

IMPACT OF NATIONAL SECURITY CONSIDERATIONS ON SCIENCE AND TECHNOLOGY

MONDAY, MARCH 29, 1982

HOUSE OF REPRESENTATIVES, COMMITTEE ON SCIENCE AND TECHNOLOGY, SUBCOMMITTEE ON SCIENCE, RESEARCH AND TECHNOLOGY, SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT,

Washington, D.C.

The subcommittees met in joint session, pursuant to call, at 9 a.m., in room 2318, Rayburn House Office Building, Hon. Doug Walgren (chairman of the Subcommittee on Science, Research and Technology) presiding.

Mr. WALGREN. On behalf of Congressman Gore and myself, I want to welcome you to these hearings. We are both pleased to co-chair these hearings as chairmen of our respective subcommittees, on my side the Science, Research and Technology Subcommittee, and on Mr. Gore's side, the Subcommittee on Oversight and Investigation.

We also want to recognize the role of Congressman Glenn English, who is chairman of the Subcommittee on Government Information and Individual Rights, who held hearings on March 10 on the proposed Executive Order on National Security Information.

In February, Congressman English and myself, and several other subcommittee chairmen, sent a joint letter to the National Security Adviser, William Clark, asking for an adequate opportunity for Congress to look carefully at any new directives on the international exchange of scientific information. Although our hearings today will focus on a number of proposals by the administration, I am afraid our discussions will be hindered by the absence of a representative of the National Security Council, which declined to provide us either with a witness or a current draft of the Executive order presently under review.

Our purpose today is to determine the impact on science and technology of recent administration proposals for increased control of potentially sensitive technology and scientific data. The proposals for tightening control over scientific exchanges, the export of technology, and the free flow of information are being put forth by the administration in the name of national security.

Now, no one would question the need to protect information of direct military importance in the interest of national security. But certainly we all have concerns that the administration may not have done a careful and comprehensive and open analysis of the total impact of the various actions on science and technology as

well as the impact on achieving economic, political, and societal goals as a whole.

Both security and scientific issues are complex and difficult. Scientific censorship is an anathema to a free society, but certainly circumstances do dictate that we find a solution to the balance we must strike between national security and the exchange of scientific and technical information. This balance is critical to safeguarding and maintaining the quality of academic research and industrial competitiveness in the United States.

Unnecessary and overly restrictive barriers to scientific communication in the international arena would, by its very nature, also curtail domestic exchange, even though the ultimate intent of such a policy may be strictly for national security. Thus, we must be careful to insure that such actions do not become more costly to our own vitality in science and technology than the benefits which may be realized by limiting foreign access or exchange between persons.

Moreover, whatever the theory is in restricting technological exchange, history has taught us that actual implementation by a bureaucratic organization can result in the most bizarre and arbitrary of actions. We cannot assume that the designated censors will represent the best and judicious aspects of our society.

To develop a proper balance between Government policies that enhance and those that protect critical scientific and technological information, we must first ask ourselves what we are trying to accomplish in our relations with the Soviet Union and the Eastern bloc. We could then perhaps more intelligently respond to the question before us—how, if at all, science and technology, either free or forbidden, might contribute to our national goals.

We will be anxious to learn from the administration witnesses how they plan to protect the flow of information without suppressing legitimate and necessary scientific exchange. Our country has enjoyed a bright history of innovation, and when we look at our society as a whole and see the other societies we are competing with, one of the brightest prospects in America is the fact that because of our free exchange we have made significant breakthroughs. The more our exchange of information becomes less free, the less we can count on making the kinds of critical breakthroughs that may be very important in every sense of our national interest.

We will also be interested in the process used to coordinate policy decisions among the various executive branch agencies responsible for national security, and the extent to which guidance was sought from the scientific and industrial communities, including the Science Adviser to the President. So, we have a wide range of ground that we would like to cover, and we certainly appreciate the witnesses here today.

I want to recognize the cochair of these hearings, Congressman Gore, the chairman of the Oversight and Investigations Subcommittee of the Committee on Science and Technology, for his comments.

Mr. GORE. Thank you very much.

The United States has long enjoyed the benefits from the competitive edge it possesses in vast areas of science and technology. Almost every aspect of our lives has as well become increasingly

tied to the course of scientific and technological advancement, including most importantly our national security.

It has been argued by some that unrestricted exchange of scientific information is central to a free society and to scientific advancement as well. While accepting the general idea of free exchange of information, others have argued that certain situations may involve the transfer of information which can have an impact on national security, and that such information flow should be restricted.

The issues which are the subject of our hearing today are both difficult and sensitive. They probe the very life force of a democratic society such as ours—freedom of speech and freedom of information, as well as how to safeguard this freedom.

Our witnesses today will help to more clearly identify the interest at stake and the potential points of conflict and, by doing so, will hopefully assist in the process of finding an appropriate balance for a free society.

As I mentioned, the United States has been at the forefront of technological innovation. The Soviet Union, however, has also benefited from Yankee know-how and ingenuity through open scientific exchange with the United States and, more often than not, by availing itself of the generally unrestricted access to information citizens of this country enjoy. Recent actions of the administration have been designed to affect greater control over the flow of information, technology, materials, and individuals than has previously existed. These actions include revisions in the wording and implementation of export control regulations and in proposed revisions to the Executive Order on National Security Information which strengthen and broaden authority to restrict dissemination of information.

The restrictions derived from these policy decisions are aimed at the free flow of technological information as well as products of technology. Such actions deserve our careful attention, and there is a need to assess whether these measures will have unintended and serious side effects.

Mr. Chairman, I am glad to welcome our first witnesses here this morning, and I wanted to take special note that Mr. Millburn and Mr. Brady and Admiral Inman have provided testimony because of our request. As a member of the Intelligence Committee, I wanted particularly to welcome Admiral Inman and advise my colleagues who have not had the opportunity to work with him in such a forum that he has an unusual degree of respect among the Members of Congress.

As I told you in a private conversation, Admiral Inman, the perception of your statement which occasioned this hearing most directly I think was somewhat uncharacteristic of the relationship you have had with the Congress and the public generally, and as I told you at that time, I am looking forward to an opportunity to explore exactly what the issues are here.

Thank you, Mr. Chairman.

Mr. WALGREN. Thank you, Mr. Gore.

I would like to recognize Congressman Brown for any opening comments.

Mr. BROWN. I have no comments.

Mr. WALGREN. We will, without objection, keep the record open at this point for other statements that members of the committee who may not be able to be here right now might want to submit.

I would like to turn to the first panel, made up of Admiral Inman, the Deputy Director of the Central Intelligence Agency, and the Honorable Lawrence Brady, Assistant Secretary for International Trade Administration in the Department of Commerce, and Dr. George Millburn, the Acting Deputy Under Secretary for Research and Engineering in the Department of Defense.

Gentlemen, we are very pleased you are here today. It is my understanding we are going to try to keep the opening remarks to something in the range of 10 minutes, if that is acceptable. Your written statements will be made a part of the record automatically.

Let's start with Admiral Inman and then go from there in either summarizing or presenting your thoughts to the committee in whatever way you feel is most effective.

STATEMENTS OF ADM. BOBBY R. INMAN, DEPUTY DIRECTOR, CENTRAL INTELLIGENCE AGENCY; HON. LAWRENCE J. BRADY, ASSISTANT SECRETARY, INTERNATIONAL TRADE ADMINISTRATION, DEPARTMENT OF COMMERCE; AND GEORGE MILLBURN, ACTING DEPUTY UNDER SECRETARY FOR RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE, ACCOMPANIED BY LEO YOUNG, DIRECTOR OF RESEARCH AND TECHNICAL INFORMATION; AND FRANK KAPPER, DIRECTOR OF MILITARY TECHNOLOGY, OFFICE OF INTERNATIONAL PROGRAMS AND TECHNOLOGY

Admiral INMAN. Thank you, Chairman Walgren and Chairman Gore.

I appreciate the opportunity to appear before this committee this morning and to expand on my previous public remarks, where I undertook on a personal basis as a knowledgeable citizen to serve as a "goad," and I am here to play that same role again here today.

If I may, I would like to enter for the record, in lieu of a formal statement, a summary of the remarks I made before the American Association for the Advancement of Science, as contained in a publication called Science News.

I had not previously known of the publication or of its reporter, but I would particularly like to call it to your attention for two reasons: One, for the short, accurate summary of views at that symposium, and second, as a plug for accuracy. It is the only reporting that accurately reflected what was said on that occasion, as you will see when you peruse the document.

Mr. WALGREN. Without objection, that will be entered in the record. I can guarantee you that no one more appreciates the divergence from accurate reporting than Members of Congress.

[The information follows:]

[From Science News, Jan. 16, 1982]

SILENCING SCIENCE FOR SECURITY

During the next decade, scientists may face greater restrictions on the dissemination of research results, said Admiral Bobby R. Inman, deputy director of the Central Intelligence Agency, last week. Inman suggested that one solution to the prob-

lem of balancing the needs of national security and science lay in including within the peer review process the question of potential harm to the nation.

The threat to scientific freedom may come from growing congressional and public awareness that the bulk of the new technology used in the buildup of Soviet defense capability was acquired from the United States or its allies, said Inman. "It is not easy to create workable and just solutions that will simultaneously satisfy the wide-ranging needs of national security and science, but I believe it is necessary before significant harm does occur, which could well prompt the federal government to overreact," he warned.

Inman presented his personal views during a panel discussion at the annual meeting of the American Association for the Advancement of Science. He said this symposium is an appropriate place to "remember that national security and scientific interests can best be advanced through a joint effort."

However, many scientists have been concerned about possible restrictions on publication of their results. The day after the symposium, the Council of the AAAS adopted the following resolution as policy: "Whereas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and of the scientific process, be it resolved that the American Association for the Advancement of Science opposes governmental restrictions on the dissemination, exchange, or availability of unclassified knowledge."

Leonard M. Rieser, chairman of the AAAS Committee on Scientific Freedom and Responsibility, told Science News, "What we see is the risk of stifling the scientific and technological community, with a certain objective in mind, and through the process weakening that community and weakening national security."

At the symposium, panelist Peter J. Denning, president of the Association for Computing Machinery, said that if the United States lessens its free flow of scientific information, economic losses will greatly outweigh reductions in national security risks. "The export control laws are an attractive vehicle for extending the government's protective influence because it is easy to argue that publication in international journals is a form of export," he said.

The administration is very concerned about the loss of technology to the Soviet Union, and the matter is being addressed by a number of departments and agencies, said George A. Keyworth II, president science adviser. "There is no consideration being given to any mandatory program of government review of scientific papers," he said.

As a model of a "reasonable and fair" approach to the problem, Inman gave the example of the voluntary review of cryptologic research (SN: 10/17/81, p. 252) that was established while he was director of the National Security Agency (NSA). Researchers working in the area of cryptology send manuscripts to the NSA for prepublication review. So far, 25 papers have been submitted, and none has caused the NSA any security concerns.

Scientific societies should follow the lead of the American Council on Education, which proposed the Public Cryptography Study Group, Inman suggested, and establish dialogues with pertinent government agencies to define problem areas. He listed examples of other fields where publication of technical information could affect national security in a harmful way: computer hardware and software, other electronic gear and techniques, lasers, crop projections and manufacturing procedures. He added that basic research has rarely presented problems for national security like those posed by applied science.

Rieser, however, was concerned "about the way one thing leads to another and finally develops into inappropriate scientific censorship." He said it is very difficult to keep scientific breakthroughs secret, and worried about the tendency to lump science and technology together.

Legislated solutions are likely to be more, rather than less, restrictive than the suggested voluntary review systems, Inman said.

One example of restrictive legislation is H.R. 109, a bill introduced a year ago in the U.S. House of Representatives that amends the Arms Export Control Act to authorize the Secretary of Defense to prescribe regulations that specify information to be protected from disclosure. The Council of the Association for Computing Machinery argued that the legislation would threaten to silence or inhibit research and development of computing technologies.

Mary M. Cheh, a George Washington University law professor, concluded her presentation on the issue: "Suppression generates hostility and mistrust, invites legal challenge, and neglects a broader conception of national security which recognizes that unfettered scientific research benefits us all."

Mr. GORE. Mr. Chairman, I think it would also be appropriate, without objection, to put the text of the statement itself in the record. (See appendix, Papers presented at Symposium on "Striking a Balance: Scientific Freedom and National Security", 1982 Annual Meeting of the American Association for the Advancement of Science, Washington, D.C., p. 230–237.)

Admiral INMAN. Thank you, sir.

As you will note, those were my personal views. They did not represent those of either the administration or the intelligence community, and that is the same situation which prevails today. I deliberately have not coordinated my remarks with either of my colleagues that are here, so we come to you as independent representatives in a forum to provide you with both information and hopefully some useful ideas.

In an open society, there is a tendency to automatically take the view that one cannot debate the substance of issues unless you see the evidence. But when one is dealing with the product of collection against a massive Soviet effort, it is difficult to convey the sense of the knowledge without revealing how we got that knowledge, and it is going to be critical in the months and years ahead that we retain that ability to collect.

I have been hard at work, nonetheless, in trying to draw from the intelligence community an unclassified summary of our knowledge of Soviet efforts to obtain Western technology, and use it ultimately to improve their own military capabilities. I have gotten several suggested statements, but they contain, in my view, too little fact to engage the concern of the public as it needs to be engaged. There is a final version that I have looked at over the weekend and it is about ready to go. With the interest of the committee, I will forward to you, hopefully within the next week or 2 weeks, a summary of the unclassified intelligence from a community perspective, not just CIA, which you may find helpful as you continue to consider this overall issue. (See appendix—Soviet Acquisition of Western Technology, April 1982; see p. 159–174.)

Mr. GORE. Mr. Chairman, I would ask unanimous consent that we hold the record open for inclusion of that material, but I must note for the record also, Admiral Inman, again as I told you in a private conversation, I have pursued the classified version of this data at some length in the Intelligence Committee and I think if the classified version were made public, it would still fall short of the so-called tidal wave that was referred to. But we can pursue that later.

Admiral INMAN. Thank you.

Let me try to summarize in aggregate for you the kinds of problems we deal with, and then let you focus your hearings as you choose on various elements of it.

As we look at the militarily useful, militarily related technology which the Soviets have acquired from the United States, principally from the West, I would roughly categorize about 70 percent of that acquisition as having been accomplished by the Soviet intelligence services. You may well have a representative of the services present this morning, and if you can get their testimony you might get a more accurate percentage. But in the absence of that, I'll give you about 70 percent as a reasonable figure to use.

The bulk of that is concentrated on trying to get directly military hardware, either through direct espionage, through open purchase and, if not successful, then illegally, of actual components or designs, and a very thorough vacuum cleaning of anything available in the public sector which will let them concentrate their espionage activities.

Of the remaining 20 to 30 percent of the acquisition of information of value to the Soviets, a small percentage comes from the direct technical exchanges conducted by scientists and by students.

The concentration by the Soviets has been on illegal trade diversions and collection directly against defense contractors and high technology firms working in advanced technology, both classified and unclassified, foreign firms and subsidiaries of U.S. firms abroad, and international organizations with access to advanced and/or proprietary technology. They are placing a high priority on the collection of science and technological information, on lasers, particle beams, and genetic engineering. They are also stepping up their efforts to acquire new and emerging technologies such as very high-speed integrated circuits and very large-scale integration technology from Western universities and commercial laboratories for both military and commercial applications.

If we are successful in efforts over the next several years to improve our counterespionage activities in this country, we will deal with the large aggregate of Soviet success in acquiring technology in the country, and that, as I understand it, is a totally separate issue from the one you're addressing this morning. But from past practice, we can be certain that as those counterespionage activities become more effective in cutting off the most lucrative source for the Soviets, they will increasingly turn their attention to the remaining elements seeking more information, seeking to mine more information, which will ultimately be of at least some value in filling the shortfalls.

Where do we think that pressure is going to come? Since the early 1970's, the Soviets and their surrogates among East Europeans have been increasingly using their national intelligence services to acquire Western civilian technologies—for example, energy, chemicals, and even consumer electronics.

Second, since the mid-1970's, Soviet and East European intelligence services have been emphasizing the collection of manufacturing-related technology in addition to weapon technology.

Third, and for this forum perhaps the most important, since the late 1970's, there has been an increased emphasis by these hostile intelligence services on the acquisition of new Western technologies emerging from universities and research centers.

In reflecting on the large body of classified information, and on the functioning, sometimes reasonably well and sometimes not well, of the Government's bureaucracy in dealing with the large outflow of knowledge, I began trying to project ahead toward that Soviet concentration which will come in greater degree on the information available from research centers and universities in the years ahead.

From my past experience, I was persuaded, and I remain persuaded, that if we can energize the academic and scientific communities to think about the problem, we have a reasonable prospect

that they will come up with innovative ideas which will not close off that flow, but will substantially lower the risks they, as citizens of this country, share with the rest of us.

Why do I feel ideas can come that will help from the academic community? Because of experience in a related topic, the field of cryptology. The Government became concerned about the public circulation of documents on cryptology. The Government's concern may well have been overdrawn, but it was nonetheless real. In the academic world there were many who were heard to say "No restriction, no dialog of any type is possible without impairment of the basic rights of academic freedom."

Some very thoughtful academicians who listened to the dialog offered to play the role of honest broker, to provide a forum to discuss in detail the Government's concerns and Government proposals. Academicians were invited to join to present their ideas. There were a few who took the view that they couldn't offer any solutions unless they saw all the evidence of a potential damage to examine.

Fortunately, there were some very able and thoughtful members of the academic community who took a different view, who were prepared to stipulate that there were national security concerns, and to try to establish mechanisms by which one could attempt to accommodate the Government's concerns without unacceptable damage to the basic tenants of academic freedom.

The American Council on Education provided the forum. The National Science Foundation underwrote the cost. The Government came forth with a series of ideas and proposals, all of which were rejected by the forum. But the academicians themselves came forward with some schemes which, on balance, seemed to offer promise. They have been implemented. They need another 18 months of use before one has a reasonable base of knowledge on which to make judgments. There is no direct relevance between the field of cryptology and the other technology outflows that we're concerned with now, and there is no certainty that the procedures which were developed for that specific model will have any relevance to the one out ahead. In fact, the chairman of the group, Chairman Mike Heyman, the chancellor at Berkeley, has been quoted as saying he does not think they are directly applicable. I have come to have such admiration for his efforts that I am prepared to accept his judgments. But I think the basic tenet is still true.

It is time for the scientific community to accept that there is an outflow of technology, that that outflow is potentially damaging, certainly to the national interest and, in specific cases, to the national security, and that they need not to wait for Government regulations but to set up their own mechanisms now to determine what they believe they can usefully contribute in the way of ideas, in the way of procedures, to limit the outflow. None of us should have any idea, to put forth any suggestion, that we will totally stop the outflow.

There will be a level of outflow that we will ultimately judge to be acceptable, but it is my judgment that the current outflow goes beyond that level, that we need to draw on the skill that the universities have already demonstrated in limiting flow when they wish to patent the results, and limiting flow when they are working for industry, to also find ways in which they can make sugges-

tions that will impede the flow to the Soviets of useful technology coming out of their own research efforts.

Ideas from the academic world will not do the job alone. The Government will also have to come up with new, responsive mechanisms to quickly respond to the scientists when they ask "will unfettered publication of research in this new area have any potential for military application in hostile areas." And if the Government is not prepared to rapidly respond and to explain why, then there would be little likelihood of the efforts on the part of the scientists ever going very far.

Let me stop at that point, Mr. Chairman, and turn the floor over to my colleagues, and then I will be prepared to answer questions.

Thank you, Mr. Chairman.

Mr. WALGREN. Thank you, Admiral Inman.

Let's turn next to Mr. Brady. Welcome to the committee, and the same introduction applies. Written statements will be made a part of the record. Please proceed as you feel appropriate.

Secretary BRADY. Chairman Walgren, Chairman Gore, I have a very short statement. I think it might be useful for the discussion that I go through it.

First let me say that we appreciate the opportunity to exchange views on what we believe in the administration is a very complex matter that we have to deal with. In addressing this topic, I will describe the issues, including the applications of our current controls and the general manner in which we are proceeding to address these issues.

Among the transfer of technology issues of concern to this administration is how and when to prevent or delay the dissemination of sensitive, dual-use technology for national security reasons without unduly burdening creative scientific research or exceeding legal limits. The complexity of this problem stems from trying to assure the proper balance between vital national security interests and the valuable process of scientific exchange.

During the enactment of the Export Administration Act of 1979, the House recognized this complexity. The Foreign Affairs Committee report stated that controlling the transfer of technology through scientific exchange is "difficult, if not impossible."

The Export Administration Act provides the statutory authority for controlling the export of U.S. technology for national security purposes. The act, like its predecessors, requires that export controls be used where necessary—

> * * * to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States.

Regulations implementing this statutory mandate have been in effect since 1955. They serve an important public purpose and the Department has a statutory duty to enforce them.

Since these controls on transfers of technology are not new, why has this issue generated so much activity in recent months? I believe there are several factors that have contributed to the expression of concern by the scientific community. First, in the past, it has not been clearly understood that our technical data regulations apply equally to all segments of society—to industry, to individuals,

and to academia. Moreover, as academic institutions have become increasingly involved in research for industrial applications, more technology becomes potentially subject to the regulations. Thus, as a consequence of academic involvement in research for industrial applications, we have become more aware of the impact on the national security of such transfers and have become more vigilant in enforcing the regulations.

The scientific community is concerned that the administration's efforts to stem the transfer of sensitive technology to potential adversaries will stifle scientific exchange to the detriment of U.S. scientific development and will impose unworkable constraints on day-to-day activities in universities.

We are not unmindful of the concerns of the scientific community, as some have suggested. Indeed, the current effort to modify our technical data regulations was prompted by the concerns of the academic community. As we try to reach a delicate balance of protecting national security without unduly impinging on scientific endeavor, we will continue to work closely with the scientific community.

I would like to describe for the members of the subcommittees how these regulations are applied currently. The Department does not control the export of technology that is already generally available to the public. Moreover, it does not restrict any nonpublic dissemination of scientific or educational data that is not "directly and significantly related to * * * industrial processes."

We focus on preventing the transfer of scientific research involving nonpublic data that is related to industrial processes and could endanger U.S. security. The Department consults with the intelligence and defense agencies in determining whether our national security could be endangered by proposed scientific exchanges. In cases where there is a national security concern, we would work with the scientists or institutions to preclude release of critical technology.

The application of export controls to scientific exchanges is illustrated by an incident that occurred under the previous administration. In February 1980, a conference on advanced computer memory technology was to be attended by representatives from the U.S.S.R., Eastern Europe, and the Peoples Republic of China. U.S. sponsors of and participants at the conference included both industry researchers and university faculty. Since the technology to be discussed at this conference included data which was not publicly available, but was related to industrial processes, nationals of proscribed countries could not participate. The sponsors restructured the conference so that the information presented would either be publicly available, or would only address general technology trends and not manufacturing processes.

I might add, Mr. Chairman, that at that point representatives from the U.S.S.R. and Eastern Europe did not attend the conference.

As academic institutions are becoming increasingly involved in research with industrial applications, this Department needs to clarify the technical data regulations to provide more specific guidance as to whom and under what conditions transfers of technology are controlled. This is not a simple process. We are consulting with

other concerned agencies, such as the CIA, Defense, State, Justice, and the National Science Foundation. At the same time we are attempting to involve the academic and industrial research communities in developing a workable set of regulations. We are also exploring ways that these communities can provide advice to the Department on a continuing basis.

This is unquestionably a sensitive and complex problem. We are striving to restrict the transfers of technology that impair our national security, while not unduly burdening scientific research. This is vital to fostering the technological breakthroughs we need in order to become more productive in today's highly competitive technology market.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Brady follows:]

STATEMENT OF LAWRENCE J. BRADY
ASSISTANT SECRETARY FOR TRADE ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE
BEFORE
HOUSE SUBCOMMITTEES
ON SCIENCE, RESEARCH AND TECHNOLOGY
AND
ON INVESTIGATIONS AND OVERSIGHT
WASHINGTON, D.C.
MARCH 29, 1982

THANK YOU FOR THE OPPORTUNITY TO EXCHANGE VIEWS ON WHAT I THINK IS ONE OF THE MOST COMPLEX ISSUES FACING THIS ADMINISTRATION -- THE APPLICATION OF EXPORT CONTROLS TO INTERNATIONAL SCIENTIFIC TECHNOLOGY TRANSFERS. IN ADDRESSING THIS TOPIC, I WILL DESCRIBE ISSUES INCLUDING, THE APPLICATIONS OF OUR CURRENT CONTROLS AND THE GENERAL MANNER IN WHICH WE ARE PROCEEDING TO ADDRESS THE ISSUES.

AMONG THE TRANSFER OF TECHNOLOGY ISSUES OF CONCERN TO THIS ADMINISTRATION IS HOW AND WHEN TO PREVENT OR DELAY THE DISSEMINATION OF SENSITIVE, DUAL-USE TECHNOLOGY FOR NATIONAL SECURITY REASONS WITHOUT UNDULY BURDENING CREATIVE SCIENTIFIC RESEARCH OR EXCEEDING LEGAL LIMITS. THE COMPLEXITY OF THIS PROBLEM STEMS FROM TRYING TO ASSURE THE PROPER BALANCE BETWEEN VITAL NATIONAL SECURITY INTERESTS

AND THE VALUABLE PROCESS OF SCIENTIFIC EXCHANGE. DURING THE ENACTMENT OF THE EXPORT ADMINISTRATION ACT OF 1979 (EAA), THE HOUSE RECOGNIZED THIS COMPLEXITY. THE FOREIGN AFFAIRS COMMITTEE REPORT STATED THAT CONTROLLING THE TRANSFER OF TECHNOLOGY THROUGH SCIENTIFIC EXCHANGE IS "DIFFICULT, IF NOT IMPOSSIBLE."

THE EXPORT ADMINISTRATION ACT PROVIDES THE STATUTORY AUTHORITY FOR CONTROLLING THE EXPORT OF U.S. TECHNOLOGY FOR NATIONAL SECURITY PURPOSES. THE EAA -- LIKE ITS PREDECESSORS -- REQUIRES THAT EXPORT CONTROLS BE USED WHERE NECESSARY

> TO RESTRICT THE EXPORT OF GOODS AND TECHNOLOGY WHICH WOULD MAKE A SIGNIFICANT CONTRIBUTION TO THE MILITARY POTENTIAL OF ANY OTHER COUNTRY OR COMBINATION OF COUNTRIES WICH WOULD PROVE DETRIMENTAL TO THE NATIONAL SECURITY OF THE UNITED STATES.

REGULATIONS IMPLEMENTING THIS STATUTORY MANDATE HAVE BEEN IN EFFECT SINCE 1953. THEY SERVE AN IMPORTANT PUBLIC PURPOSE AND THE DEPARTMENT HAS A STATUTORY DUTY TO ENFORCE THEM.

SINCE THESE CONTROLS ON TRANSFERS OF TECHNOLOGY ARE NOT NEW, WHY HAS THE ISSUE GENERATED SO MUCH ACTIVITY IN RECENT MONTHS? I BELIEVE THERE ARE SEVERAL FACTORS THAT HAVE CONTRIBUTED TO THE EXPRESSION OF CONCERN BY THE SCIENTIFIC COMMUNITY. FIRST, IN THE PAST, IT HAS NOT BEEN CLEARLY UNDERSTOOD THAT OUR TECHNICAL DATA REGULATIONS APPLY EQUALLY TO ALL SEGMENTS OF SOCIETY: TO INDUSTRY, TO INDIVIDUALS, AND TO ACADEMIA. MOREOVER, AS ACADEMIC INSTITUTIONS

97-341 O - 82 - 2

HAVE BECOME INCREASINGLY INVOLVED IN RESEARCH FOR INDUSTRIAL APPLICATIONS, MORE TECHNOLOGY BECOMES POTENTIALLY SUBJECT TO THE REGULATIONS. LASTLY, WE HAVE BECOME MORE AWARE OF THE IMPACT ON THE NATIONAL SECURITY OF SUCH TRANSFERS AND HAVE BECOME MORE VIGILANT IN ENFORCING THE REGULATIONS.

THE SCIENTIFIC COMMUNITY IS CONCERNED THAT THE ADMINISTRATION'S EFFORTS TO STEM THE TRANSFER OF SENSITIVE TECHNOLOGY TO POTENTIAL ADVERSARIES WILL STIFLE SCIENTIFIC EXCHANGE TO THE DETRIMENT OF U.S. SCIENTIFIC DEVELOPMENT AND WILL IMPOSE UNWORKABLE CONSTRAINTS ON DAY-TO-DAY ACTIVITIES IN UNIVERSITIES.

WE ARE NOT UNMINDFUL OF THE CONCERNS OF THE SCIENTIFIC COMMUNITY, AS SOME HAVE SUGGESTED. INDEED, THE CURRENT EFFORT TO MODIFY OUR TECHNICAL DATA REGULATIONS WAS PROMPTED BY THE CONCERNS OF THE ACADEMIC COMMUNITY. AS WE TRY TO REACH A DELICATE BALANCE OF PROTECTING NATIONAL SECURITY WITHOUT UNDULY IMPINGING ON SCIENTIFIC ENDEAVOR, WE WILL CONTINUE TO WORK CLOSELY WITH THE SCIENTIFIC COMMUNITY.

I WOULD LIKE TO DESCRIBE FOR THE MEMBERS OF THE SUBCOMMITTEES HOW THESE REGULATIONS ARE APPLIED CURRENTLY. THE DEPARTMENT DOES NOT CONTROL THE EXPORT OF TECHNOLOGY THAT IS ALREADY GENERALLY AVAILABLE TO THE PUBLIC. MOREOVER, IT DOES NOT RESTRICT ANY NONPUBLIC DISSEMINATION OF SCIENTIFIC OR EDUCATIONAL DATA THAT IS NOT "DIRECTLY AND SIGNIFICANTLY RELATED TO ... INDUSTRIAL PROCESSES."

WE FOCUS ON PREVENTING THE TRANSFER OF SCIENTIFIC RESEARCH INVOLVING NONPUBLIC DATA THAT IS RELATED TO INDUSTRIAL PROCESSES AND COULD ENDANGER U.S. SECURITY. THE DEPARTMENT CONSULTS WITH THE INTELLIGENCE AND DEFENSE AGENCIES IN DETERMINING WHETHER OUR NATIONAL SECURITY COULD BE ENDANGERED BY PROPOSED SCIENTIFIC EXCHANGES. IN CASES WHERE THERE IS A NATIONAL SECURITY CONCERN, WE WOULD WORK WITH THE SCIENTIST OR INSTITUTION TO PRECLUDE RELEASE OF CRITICAL TECHNOLOGY.

THE APPLICATION OF EXPORT CONTROLS TO SCIENTIFIC EXCHANGES IS ILLUSTRATED BY AN INCIDENT THAT OCCURRED UNDER THE PREVIOUS ADMINISTRATION. IN FEBRUARY 1980, A CONFERENCE ON ADVANCED COMPUTER MEMORY TECHNOLOGY WAS TO BE ATTENDED BY REPRESENTATIVES FROM THE U.S.S.R., EASTERN EUROPE AND THE PRC. U.S. SPONSORS OF AND PARTICIPANTS AT THE CONFERENCE INCLUDED BOTH INDUSTRY RESEARCHERS AND UNIVERSITY FACULTY. SINCE THE TECHNOLOGY TO BE DISCUSSED AT THIS CONFERENCE INCLUDED DATA WHICH WAS NOT PUBLICLY AVAILABLE BUT WAS RELATED TO INDUSTRIAL PROCESSES, NATIONALS OF PROSCRIBED COUNTRIES COULD NOT PARTICIPATE. THE SPONSORS RESTRUCTURED THE CONFERENCE SO THAT THE INFORMATION PRESENTED WOULD EITHER BE PUBLICLY AVAILABLE OR WOULD ONLY ADDRESS GENERAL TECHNOLOGY TRENDS AND NOT MANUFACTURING PROCESSES.

AS ACADEMIC INSTITUTIONS ARE BECOMING INCREASINGLY INVOLVED IN RESEARCH WITH INDUSTRIAL APPLICATIONS, THE DEPARTMENT NEEDS TO

CLARIFY THE TECHNICAL DATA REGULATIONS TO PROVIDE MORE SPECIFIC GUIDANCE AS TO WHOM AND UNDER WHAT CONDITIONS TRANSFERS OF TECHNOLOGY ARE CONTROLLED. THIS IS NOT A SIMPLE PROCESS. WE ARE CONSULTING WITH OTHER CONCERNED AGENCIES, SUCH AS THE CIA, DEFENSE, STATE, JUSTICE AND THE NATIONAL SCIENCE FOUNDATION. AT THE SAME TIME, WE ARE ATTEMPTING TO INVOLVE THE ACADEMIC AND INDUSTRIAL RESEARCH COMMUNITIES IN DEVELOPING A WORKABLE SET OF REGULATIONS. WE ARE ALSO EXPLORING WAYS THAT THESE COMMUNITIES CAN PROVIDE ADVICE TO THE DEPARTMENT ON A CONTINUING BASIS.

THIS IS UNQUESTIONABLY A SENSITIVE AND COMPLEX PROBLEM. WE ARE STRIVING TO RESTRICT THE TRANSFERS OF TECHNOLOGY THAT IMPAIR OUR NATIONAL SECURITY WHILE NOT UNDULY BURDENING SCIENTIFIC RESEARCH. THIS IS VITAL TO FOSTERING THE TECHNOLOGICAL BREAKTHROUGHS WE NEED IN ORDER TO BECOME MORE PRODUCTIVE IN TODAY'S HIGHLY COMPETITIVE TECHNOLOGY MARKET.

Mr. WALGREN. Thank you, Mr. Brady.

We will now turn to Dr. Millburn.

Dr. MILLBURN. Mr. Walgren, Mr. Gore, members of the committee: I am pleased to have this opportunity to testify before you on the impact of national security considerations on science and technology. With me are Dr. Leo Young, Director of Research and Technical Information in my office, and Dr. Frank Kappewr, Director of Military Technology Sharing in the Office of International Programs and Technology.

I have already submitted written testimony for the record, and I would like now to just make this very brief statement.

We are currently looking into the whole process of technology export controls as they affect our national research endeavor in general, and our universities in particular. We have instituted dialogs with the universities, with educational and research associations, and with professional technical societies, and are about to fund a study of the problem by the National Academy of Sciences. We are doing all these things both to guide our actions more wisely and to enlist the wholehearted support of the research community.

Over the years there has been a shift in emphasis from product control to control of technology, as such. This shift has complicated DOD's relationships with the universities since a considerable amount of relevant, high-technology knowhow exists, not only in those industrial firms where the knowhow is applied, but also in the universities. A basic tension, therefore, exists between the requirements of national defense and the need for universities to remain relatively free in their pursuit and dissemination of knowledge.

Best Available Copy

Industry is driven by goals and motivations quite different from those found in the university, and proprietary restraints act to inhibit the flow of the really important knowhow. In academia, on the other hand, prestige and recognition are attained by being the first to publish a new idea or concept. It is, therefore, crucial that the Department of Defense be sensitive to these differences in its pursuit of the control of the export of technologies that are critical in a military sense.

The situation is being complicated by, first, the changing nature of military technology. Military power is now highly dependent on advanced commercial technology.

Second, the changing interests of university researchers. Universities have entered a new era in which applied research—for example, in genetic engineering—is receiving pronounced attention.

Third, the emerging concept of militarily critical technology. The Department of Defense has spent a great deal of time and effort defining what technologies or knowhow would substantially benefit potential adversaries.

Except for a few academic consultants to the Department, the academic community has little knowledge or appreciation of the struggle within DOD to better define what technical information is important militarily and should be subject to some form of review and ultimately of control.

We are caught in a dilemma. If we vigorously attempt to regulate the flow of scientific information in the scientific community, it could jeopardize the strength and vitality of the very community we are seeking to revitalize for the sake of national defense. On the other hand, if we abandon any attempt at regulation in the university context, it could seriously compromise and undercut other efforts to control the outflow of militarily-critical technology.

Nonetheless, there is reason for some optimism. We have attempted to at least lay a framework for solving the issue by means both practical and, it is hoped, acceptable to the academic community. A dialog with the universities has already begun over the transfer of nonclassified but nonetheless sensitive information in the very high speed integrated circuit program.

The problem of controlling the flow of sensitive information may not be as difficult as first perceived. The situation is similar to that of proprietary information developed in the course of industrially-funded university research. A corporation supporting university research is not concerned when a professor teaches basic science in engineering in the classroom. If, however, in the course of his research under corporate contract the professor made public information could, in essence, benefit a competitor, there would be cause for alarm. The information which could help a competitor is, in general, manufacturing or process knowhow, not basic science and technology.

The focus of DOD attention for the near future will be toward establishing clear and consistent guidelines for the release of information in DOD-university contracts. An outline of some considerations is given in the written testimony which I have already submitted.

Toward this end, we have already met with and started an exchange of views with non-DOD organizations involved in research.

Following a recommendation of the Defense Science Board, a DOD-university forum has been set up. It consists of eight university presidents, the heads of three university and higher education organizations, and nine members representing the Department of Defense. The first meeting was held on February 24.

This forum will consider several areas of mutual concern. The first meeting dealt mainly with the question of export control. A working group to further define and understand this problem is now being set up with the help of the Association of American Universities.

We are also commissioning a study to be performed by the National Research Council on the broader question of the effects of export control on the publication and dissemination of technology.

In conclusion, we are tackling a serious and difficult problem that has been ignored for too long, and we are tackling it in a responsible way. We do not want to kill the goose that lays the golden eggs. We just don't want the eggs to fall into the wrong hands. I believe we are all agreed on that.

[The prepared statement of Dr. Millburn follows:]

NOT FOR PUBLICATION UNTIL
RELEASED BY THE COMMITTEE

STATEMENT ON

IMPACT OF NATIONAL SECURITY CONSIDERATIONS

ON SCIENCE AND TECHNOLOGY

BY

GEORGE P. MILLBURN

ACTING DEPUTY UNDER SECRETARY OF DEFENSE

FOR RESEARCH AND ENGINEERING

(RESEARCH AND ADVANCED TECHNOLOGY)

BEFORE A JOINT SESSION OF THE

SCIENCE, RESEARCH AND TECHNOLOGY SUBCOMMITTEE

AND THE

INVESTIGATIONS AND OVERSIGHT SUBCOMMITTEE

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY

OF THE

HOUSE OF REPRESENTATIVES

97TH CONGRESS, SECOND SESSION

29 MARCH 1982

Best Available Copy

Mr. Chairman, Members of the Committee:

I am pleased to have this opportunity to testify before you on the Impact of National Security Considerations on Science and Technology. With me are Dr. Leo Young, Director of Research and Technical Information in my office, and Dr. Frank Kapper, Director of Military Technology Sharing in the Office of International Programs and Technology.

This committee has a special concern shared by the Department of Defense for the health and vigor of Science and Technology R&D especially at the universities, where approximately one R&D dollar in seven in FY 1982 comes from spending for defense. Most of the results of U.S. research is shared freely with the rest of the world, and improves the quality of life of people in all countries. Our open policy with regard to publishing research results also benefits this country in most cases in that it speeds the dissemination of new knowledge and its application to innovative new products. Unfortunately, some technologies have critical military applications of which the researcher may be unaware, and may be turned against us when research results for which we have worked and paid fall into the hands of declared or potential enemies. It is clearly detrimental to the national security when this happens, and it is important to prevent that kind of technology from being exported to unfriendly or unreliable countries. In applying any such controls one must be very careful not to disturb or interfere with the finely tuned research apparatus of which the universities are such a key component lest we throw out the baby with the bath water.

Some idea of United States leadership in technology may be guaged from the fact that U.S. license and royalty receipts from foreign sources were nine times higher in 1978 than what the U.S. pays for foreign licenses and

royalties ties (Science Indicators 1980, Page 228). The corresponding figure for Japan is only 0.22 and for the Federal Republic of Germany it is 0.4. For Britain and France it is close to unity, i.e., almost in balance. Only the United States, often to its detriment, exports through licenses and royalties nine times as much technology as it receives. (There is a lengthy and revealing analysis of the situation in a thirteen-page advertisement by the Japanese Government in the October 1980 issue of Scientific American.)

The Department of Defense is currently looking into the whole process of technology export controls as they affect our national research endeavor in general and our universities in particular. We have instituted an active dialogue with the universities, with educational and research associations, and with professional technical societies, and are about to fund a study of the problem at the National Academy of Sciences. We are doing all these things both to guide our actions more wisely and to enlist the wholehearted support of the American research community by communicating clearly to them our concerns.

Let me summarize for you now how export controls operate at this time. I shall follow the discussion in the report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements.

1. EXPORT CONTROLS

Control of exports, including technical data, is centered in two Departments of the U.S. Government, State (which exercises control of military hardware and technology) and Commerce (which has cognizance of commercial commodity control and dual-use technology). DoD and other appropriate departments are required to identify goods and technology for inclusion on control lists.

The State Department, under Section 38 of the Arms Export Control Act, has issued regulations restricting the "export" by "oral, visual, or documentary" means of certain information, data, and equipment to foreign nationals. These restrictions, known as the International Trade in Arms Regulations (ITAR), rely on the following definition of "export": "Transfer of data and information to, inter alia, foreign nationals within the U.S."

The Export Administration Act (EAA) of 1979 provides authority to regulate exports, in a manner designed to minimize interference with the ability to engage in commerce. In accordance with the Act, the Secretary of Commerce maintains the Commodity Control List, a list of all goods and technologies subject to export controls. Under the act, the Secretary of Defense is given responsibility for developing a list of militarily critical technologies, with emphasis on manufacturing know-how, keystone manufacturing equipment, and goods accompanied by sophisticated operation or maintenance know-how. This list is to be used as a guide to Commerce Department licensing officers in making export determinations. A list of militarily critical technologies was developed and published in the Federal Register on 1 October 1980 as required.

Best Available Copy

The shift in emphasis from product control to control of technology (technical data, manufacturing equipment, and processes) has complicated DoD's relationship with the universities since a considerable amount of relevant high technology know-how exists, not only in those industrial firms where the know-how is applied, but also in the universities. A basic tension therefore exists between the requirements of national defense and the need for universities to remain relatively free in their pursuit and dissemination of knowledge.

Industry is driven by goals and motivations quite different than those found in the university, and proprietary restraints act to inhibit the flow of the really important "know-how." In academia, on the other hand, prestige and recognition are attained by being the first to publish a new idea or concept. It is, therefore, crucial that DoD be sensitive to these differences in its pursuit of the control of technologies that are critical in a military sense.

2. CURRENT TRENDS

Until recently, the conduct of research in the universities has not caused a significant problem with respect to the handling of sensitive defense information. Most research, even that which has been funded by DoD, is unclassified research. Classified research, on the other hand, is conducted in off-campus institutions (e.g., Lawrence Livermore Laboratory) which, although affiliated with a university, are nonetheless separate enough so that strict security procedures can be employed.

More recently the situation has been complicated by the following factors and trends.

Best Available Copy

- Changing Nature of Military Technology: Military power is now highly dependent on advanced commercial technology. To further complicate matters, much of the technology that is now useful from a military point of view is also useful in the commercial sector (computers, fiber optics, etc.). Before, research on military-specific technology was somewhat contained in government and industry laboratories and on a selected number of university campuses. Now, with the pervasiveness of high technology throughout military systems, the balance has shifted. With few exceptions, the development of high technology, whatever the source, has military impact.
- Changing Interests of University Researchers: Universities have entered a new era in which applied research in certain fields is receiving pronounced attention. For example, in genetic engineering, high technology companies are being spun off from the universities to conduct proprietary applied research and commercialize the results.
- Emerging Concept of Militarily Critical Technology: The DoD has spent a great deal of time and effort defining what technologies are important, militarily, and what transfer of information or "know-how" would substantially benefit potential adversaries. The Militarily Critical Technologies List (MCTL) is more general than either ITAR or Export Administration Regulations (EAR) in terms of technology know-how and is more oriented toward manufacturing processes

> Although the list attempts to define and delimit areas of technology, it contains over 620 technology titles with literally thousands of critical elements specified under those titles. This coverage is a function of the two basic criteria for inclusion on the MCTL: military significance and adversary capability. The MCTL is a detailed and structured technical statement of development, design, production, and utilization technology which DoD considers to be critical to a given military capability and of significant value to potential adversaries. The MCTL is a technical reference and source document and not a control list.

Except for a few academic consultants to DoD, the academic community has little knowledge or appreciation of the struggle within DoD to better define what information, technologies, and critical elements are important militarily and should be subject to some form of review and ultimately of control. Except for the publication of the MCTL titles in the Federal Register on October 1, 1980, there has been little guidance to the academic community on what technologies are considered sensitive and why they should be guarded. This lack of guidance has led to some consternation on the part of the academic community, since the MCTL titles interpreted broadly could cover a breadth of technology DoD did not intend to be subject to controls.

DoD is caught in a dilemma. If it vigorously attempts to regulate the flow of scientific information in the scientific community, it could jeopardize the strength and vitality of the very community it is seeking to revitalize for the sake of national defense. On the other hand, if DoD abandons any

attempt at regulation in the university context, it could seriously compromise and, in certain cases, totally undercut other efforts to control the out-flow of militarily critical technology.

The middle ground is a difficult one to establish. We have attempted, if not to solve the problem, to lay a framework for solving the issue by means both practicable and, it is hoped, acceptable to the academic community. A dialogue with the universities has already begun over the transfer of non-classified but nonetheless sensitive information in the Very High Speed Integrated Circuit (VHSIC) Program.

3. DOD GUIDELINES

The university research that DoD considers militarily critical is for the most part DoD-funded. DoD targets research funds to those areas of basic research with potential for military application. Other federally-funded research (NASA, NSF, DoE, HHS) could have military potential but the proportion of research in this category would be much smaller than that which is funded by DoD. Non-federally-funded university research with military applicability is an even smaller component of university research.

As to that research funded by DoD, the department increasingly is attempting to monitor for national security purposes the flow of information and technical data emanating from the research. This regulation is currently applied in certain areas of research performed by DoD, DARPA, and the Military Departments.

The Air Force, for example, has implemented certain procedures for restricting the flow of unclassified technical information which nonetheless falls

under the category of information subject to export control. All documents in this category generated by Air Force personnel or under Air Force contracts must carry the following warning:

> SUBJECT TO EXPORT CONTROL
>
> This document contains information for manufacturing or using munitions of war. Export of the information contained herein or release to foreign nationals within the United States, without first obtaining an export license, is in violation of the International Traffic in Arms Regulations. Such violation is subject to a penalty of up to 2 years imprisonment and a fine of $100,000 under 22 U.S.C. 2778.

The focal point for control is the DoD contract; the Government negotiates the terms of the release of information with the contractor. The Project Office or Contract Monitor within DoD thus becomes the interpreter of military criticality and the extent to which ITAR or EAR is applicable. The system is voluntary in the sense that the contract does not have to be accepted. If guidelines for release of information are accepted as part of the contract, then there should be little room for misunderstanding later.

It could be argued that restrictions such as these violate the spirit of academic freedom and will curtail the free flow of information required for maintaining a healthy dialogue within the scientific community. This might be true if DoD were seeking to restrict the flow of all scientific information

Best Available Copy

Available Copy

directly or indirectly related to military capability. This, however, is clearly not the case. The Department of Defense is assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research.

The situation is similar to that of proprietary information developed in the course of industrially-funded university research. A corporation supporting university research is not concerned if a professor teaches basic science and engineering in the classroom. If, however, in the course of his research under corporate contract the professor made public information which could in essence benefit a competitor, there would be cause for alarm. The information which could help a competitor is, in general, manufacturing or process know-how, not basic science and technology.

The focus of DoD attention for the near future will be toward establishing clear and consistent guidelines for the release of information in DoD-university contracts. This policy should be standardized for all DoD agencies and the Services so that the universities and individual scientists will not have to cope with uncertainties arising from alternate interpretations or diverging opinions from different DoD agencies. DoD, must eventually set up some mechanism for establishing and implementing a DoD-wide policy.

4. SOME OPTIONS UNDER CONSIDERATION FOR DOD-FUNDED UNIVERSITY RESEARCH

The Defense Science Board Task Force has presented the following options which are now under active consideration.

- o DoD could immediately implement an internal process whereby a committee of R&D experts in OSD and the Military Departments

could meet in order to work out mutually acceptable terms for reviewing university research contracts. This process must take place with appropriate consultation with the universities.

- DoD should seek the concurrence of State and Commerce in implementing these guidelines where the DoD Project Manager or Contract Monitor negotiates with the university contractor over what information is releasable and what might be subject to ITAR and EAR.
- In the course of the contract work, pre-publication review would allow for a contractor to change or modify the presentation of technical data so that it would be releasable to the public without going through the licensing process. Pre-review could in a sense be DoD's mechanism for interpreting ITAR for the universities and may be less onerous than requiring universities to submit formal license requests to State (ITAR) or Commerce (EAR). It informs the publishers of the Department of Defense position which, because of the advisory and concurring role of the Department, is likely to be adopted by the Office of Munitions Control.
- In practice, a time limit could be imposed such that the investigator would be allowed to publish his results if, after informing the Government, he has not received a response within a designated period (30-60 days).
- Only in those cases where the information is clearly deemed subject to ITAR/EAR would a license be sought. DoD cannot

exempt university research from ITAR. There are no provisions for ad hoc exemptions or arrangements to change the ITAR requirements for individuals or groups including the universities.

- The review process could be simplified further if DoD first addressed the most critical and time-urgent technologies and then proceeded to wider coverage.

If such a plan were implemented, the universities would be assured that DoD is not seeking a broad restriction on the flow of scientific information within the university community which would be against DoD's own interest. The effort would be focused and therefore limited since:

- DoD-funded research constitutes only a part of the overall university research budget.
- Within DoD-funded unclassified research, only manufacturing and process-oriented research (as opposed to basic research) are of concern.
- Even with process-oriented research certain information could be released generally to the scientific community after thorough review.
- Even information which could not be released publicly could be circulated within a selected subgroup of the scientific community.

If the review and control process were centered initially around the DoD contract and the relationship between the DoD Contract Monitor and the university contractor, it would greatly simplify the paperwork.

- The university and the individual scientist would know in advance what was expected in terms of information release. The policy could be clearly articulated.

Best Available Copy

- The export control/release of sensitive information guidelines would simply be an add-on to the existing contract procedures.
- The Departments of State and Commerce would not be flooded with unnecessary license requests from the university sector.
- Those license applications received from the university sector would be more focused and therefore more substantive since they would have already passed through a process of review of the military significance of the data release.
- Judgment as to what is militarily critical would remain with DoD.
- The system could operate with personnel and structures already in place at DoD, State, and Commerce. It might require some additional staffing to assure that the review process is carried out expeditiously, but would not require an extensive expansion on the part of any one of the agencies and/or creation of a new bureaucracy.

Concerning foreign nationals, DoD's primary interest is to exclude foreign students from participating in advanced research specifically related to the development of militarily critical technologies, and particularly to control foreign students from Communist countries from having access to R&D projects funded by the Defense Department. Numerous advances in Soviet military weapon systems are directly traceable to technology transfers that occurred as a result of Soviet and Warsaw Pact student and scientist exchanges and their attendance at international scientific symposia held in the United States.

Certain individuals have suggested that the responsibility for controlling access by foreign nationals to our campuses must be with the State Department

and that the control mechanism be the visa. While outright denial of a visa is an effective way of preventing foreign access to U.S. technology on university campuses, universities have generally expressed strong opposition to this use of the visa process. Visas may be granted with specific restrictions attached, however, the universities have few mechanisms for controlling the foreign students once they enter the campus, and cannot guarantee compliance with such restrictions. Given the decentralized and fluid nature of most campuses, universities are neither structured nor staffed to police the flow of visitors. The Department of Defense does support denial of visas to Communist country nationals on a case by case basis when there is not apparent benefit to the U.S. from the visit.

For highly sensitive areas of research, DoD retains its preference that no foreign nationals be assigned to conduct research, but could accommodate other mechanisms of oversight once the likelihood of ITAR - controlled data being developed in certain program elements has been established.

- Principal Investigators could be asked to assign only U.S. citizens or immigrant aliens to program elements assessed as being likely to develop ITAR controlled data; and
- Principal Investigators could be asked to limit participation in the remainder of the program to foreign nationals who have declared that they do not intend to expatriate their acquired knowledge.

5. NON-DOD-FUNDED UNIVERSITY RESEARCH

Research not funded by DoD would essentially fall in two categories:

- Federally-funded research by other agencies (NSF, NASA, HHS, DoE, etc.).

- Industry- or internally-funded university research.

The Defense Science Board Task Force discussed the following options regarding non-DoD funded university research.

Federally-Funded (Non-DoD) Research

DoD could explore with other agencies the use of contract guidelines similar to those used in DoD contracts, to be negotiated with university contractors in a manner similar to that suggested for DoD contracts. The number of contracts so regulated would be much smaller, by percentage, than DoD contracts. DoD would furnish the other federal agencies a contact person in DoD who would be supportive in the following ways:

- Determine what areas of that agency's business would fall into the realm of ITAR/EAR.
- Help word the guidelines for the initial research contract.
- Help in pre-publication review if this were deemed appropriate, in a manner similar to that outlined for DoD contract research.
- Take the burden of determining military criticality off the shoulder of the NSF, NASA, HHS, DoE Project Manager and make that the responsibility of DoD.

Except for a few cases, it is anticipated that the need and/or urgency to control non-DoD-funded university research is less than that required for DoD-funded research, since the militarily critical areas are fewer in number and the research is usually not as directly linked to process or utilization technology. Thus, it would not seriously endanger national security if non-DoD-funded research guidelines were negotiated and implemented subsequent to a full implementation of the guidelines for DoD-funded research.

An added advantage for such a graduated approach is a practical one. DoD and the universities will have gained some valuable experience in their communication over DoD-sponsored research. Furthermore, the MCTL and its impact on ITAR and EAR will have been more clearly defined. A graduated strategy does not postpone initial talks and contacts with other agencies over this matter, but merely anticipates what sort of time frame would be required in order to implement a full control program.

It is also possible that a peer review mechanism similar to that adopted for cryptography research may be applicable to basic research funded by agencies other than DoD. This method seems to be working well.

Non-Federally-Funded Research

A significant amount of basic research is funded by sources other than the Federal Government, including industry, foundations, and private individuals. We cannot now tell whether any of this research or what proportion of this research might fall into the category of militarily critical and/or be subject to control by ITAR/EAR. Since the Federal Government has no contractual ties, the use of the federal contract or grants as a point of control is not feasible. Voluntary controls and peer review may, however, be possible since the university is still subject to ITAR and EAR whether or not research is federally contracted.

DoD could essentially play the same role as previously, i.e., as consultant and advisor as to what is militarily critical and subject to ITAR and EAR. Universities would still be obliged to submit license application if determination is made that research is subject to control, but these instances could be expected to be few in number since the research itself would have already passed through a filter of military criticality as defined by DoD.

Although DoD's role as an advisor would be the same as that constructed for non-DoD federally-funded research, the mode of approach, the persons and institutions involved, and the process itself could be quite different.

DoD could initiate a dialogue with the university community through its organizational representatives (e.g., Association of American Universities) concerning the magnitude of the problem and, if needed, by the structuring of a peer review process for the control of technical information of a sensitive nature which is the result of research not funded by the U.S Government. Peer review could be in the form of ad hoc committees established by discipline, or more formally, by instituting a review committee within the framework of scientific societies (IEEE, AIAA, ACS, etc.).

Through this forum, the DoD could negotiate a satisfactory resolution of three of the more important elements of any control process.

- Determination of Research Subject to Review: DoD, with its considerable experience in defining the MCTL, could relate its concerns to the academic community and attempt to define a mutually acceptable categorization of research areas that would be recognized as militarily critical, but not contractually subject to the review processes previously discussed. These would no doubt include the dual-use technologies which have both high military and high commercial payoff.
- Specific Guidelines for Selected Research Area: DoD could meet with representatives from the university community, including the scientific societies, to discuss what guidelines would be appropriate for a particular discipline.

- Pre-Publication Review: From a constitutional point-of-view, this is the most sensitive area and one which DoD should approach with utmost caution. An overly ambitious program of information control could easily end up in the courts. The emphasis here should be on:
  - the voluntary nature of the program,
  - the principle of peer review,
  - some mechanism for appeal if a particular researcher feels that guidelines have been unfairly applied,
  - time limit for response. If the Government has not responded in 30-60 days, the investigator can assume there is no prob'em with publication of the results.

6. CURRENT PROGRESS AND SUMMARY

The key to a successful export control is an understanding by the university community and by DoD of each other's needs. We must therefore first educate one another. In federally-contracted research programs, the contract negotiation process itself could provide a vehicle for educating the university research community of the needs of DoD for restricting information in certain sensitive areas. Even in areas of research where there is no formal government contract relationship, there could be a form of education through osmosis since research guidelines would be, in most cases, available to the public, and since there is already a substantial flow of information between academics.

There may be a few areas of research of high priority where DoD may wish to catalyze some sort of peer review process similar to that undertaken in

the field of cryptography. The need for an extensive peer review program is not immediately apparent and the mere publication of clear DoD guidelines may solve the problem.

A key to any voluntary program is communication. Some of the fears within the academic communities could be alleviated if DoD could make public the description, including critical elements, of those technologies which it considers militarily critical. The document that contains these and the justifications for why these technologies are considered critical is classified SECRET. The promulgation of an unclassified version of the MCTL would help immensely.

Table 1 shows schematically how DoD could function as a catalyst and advisor and, in certain cases, an arbitrator in a framework where ITAR/EAR is the legislative umbrella. The plan is structured to utilize existing personnel and avoid the creation of a new bureaucracy. It can be accomplished with no additional legislation since it represents only one interpretation of current law and/or the extension of current practice. It is staged in phases that allow DoD to control its own contracts first (Phase I), and then extend to other areas (Phases II and III), with the benefit of the experience derived in Phase I.

We have begun meetings and an exchange of views with non-DoD organizations involved with research. Following a recommendation of the Defense Science Board Task Force, a DoD/University Forum has been set up. It consists of eight university presidents, the heads of three university and higher education organizations, and nine members representing DoD. The first meeting was held last month. The forum will consider several areas

TABLE 1

A PHASED PROGRAM TO DEVELOP GUIDELINES

FOR RESEARCH SUBJECT TO ITAR/EAR COVERAGE

	PHASE I	PHASE II	PHASE III
	DoD Funded Research	Non-DoD, Federally-Funded Research	Industry/University and Internally Funded Research
Guidelines for dissemination of technical information	• Written into all contracts	• Written into some contracts as deemed appropriate by inter-agency task force (to be instituted)	• Used as needed in peer review process
Implementation	• Immediate set-up DoD-Service wide task force to formulate department-wide policy. • Coordinate policy with State/Commerce	• Initiate Dialogue with all other Federal Agencies concerning extent and specifics of contract coverage • Implementation of guideline coverage could begin after that of Stage I	• Initiate dialogue with university representatives and science societies about extent of problem and possible peer review structure • Highlight only areas which are clearly not covered in Stage I and III • May not have to be implemented
DoD Involvement	• DoD primary actor	• DoD institutes proc[illegible] and formulates contract [illegible] for aid in implementing guidelines, [illegible]	• DoD catalyzes a process and plays advisor role only in peer review

Best Available Copy

of mutual concern. The first meeting dealt mainly with the question of export control, and a working group to further define and understand this problem is now being set up with the help of the Association of American Universities. We are also commissioning a study to be performed by the National Research Council on the broader question of the effects of export control on the publication and dissemination of technology by professional societies as well as on the conduct of research at the universities.

In conclusion, we are tackling a serious and difficult problem that has been ignored for too long in a serious and responsible way. We do not want to kill the goose that lays the golden eggs. We just don't want the eggs to fall into the wrong hands. I believe we are all agreed on that.

Mr. WALGREN. Thank you, Dr. Millburn.

The Chair recognizes Mr. Gore.

Mr. GORE. Thank you very much, Mr. Chairman.

Admiral Inman, this subject is one that is very difficult to treat, as I'm sure you probably know at this point as well as anyone. The purpose of these hearings is not to say to you and others at the witness table that there is no balance and there is no legitimate concern being expressed, but rather to elevate the degree of consideration given to academic freedom and to make you more keenly aware of the importance the American people place on protecting academic freedom.

When I hear you say that you want to serve as a goad to discussion, I can understand that. And when you say you want to energize the academic community to take these concerns seriously, I can understand that. When you say you want them not to wait for the Government to act, then I think you begin to cross a line that may not exist. I think you begin to cross a line that the Government should approach very, very cautiously.

You don't want to engender the fear in the academic community that the Government will, in fact, impose some burdensome censorship if they do not take the suggestions you offer as a goad, and as two subcommittees of the Congress, I believe that we reflect the views of the American people that yes, this is a problem that requires a balanced and sensitive approach, but no, we don't want to even take the first step along the road that has made Soviet science so pitiful, which is essentially the censorship and restriction that has inhibited their advancement.

Admiral INMAN. I really just must reject the last phase as being applicable in this case. The question of determining how one restricts flow, that to take that on you somehow are going to create a science and technology world like the one of the Soviet's, I think is just not a fair comparison to which any reasonable interpretation of my remarks would lead you.

In the interest of goading the Congress as well as the public, let me turn to Chairman Walgren's opening remarks, which convey to

Best Available Copy

this listener a sense that anything related to an exchange is good and anything which would impinge on that exchange is not good. I think you have a responsibility now to look at the question of what benefits have accrued to the United States from the exchanges of the last 13 or 14 years? Have we, as a society, measureable benefits from our exchange with the Soviets across the whole range that would cause us to say a continued outflow to help build up their technology is worth doing? If there's a case there, then you probably could alter my attitude.

But I am no longer prepared to accept, as a given, that the U.S. benefits from that exchange to the degree that we should not, in fact, consider ways to impede that flow.

Mr. GORE. Well, let me continue my questioning.

First, in reaction to that, I don't think that the national security apparatus of the Government can shift the burden of proof to the academic community and require them to justify continued freedom.

Admiral INMAN. Again, Mr. Gore, I don't think you can characterize "continued freedom" as the question that we're talking about. We have innumerable ways in this society in which we work with constraints, but that does not give up freedom. It controls the degree to which one parcels it out. My enormous distress with earlier coverage by the press, as with this, is to cast it in black-and-white issues that freedom is at risk on one side as opposed to some nebulous kind of concerns about Soviet gains on the other. I think that unfairly casts, for those of us who are in the process of watching the Soviet events, how one might advise the Government to react to it.

Mr. GORE. Well, I know you to be a very sensitive analyst and capable of very subtle thought, and I want my reaction to your proposal to be fair and balanced and not an overreaction.

Nevertheless, in discussing the absolute principles and values that conflict one with the other in this arena, it is impossible to avoid stating one's concerns without occasional reference to the absolute value one is seeking to protect. In the case of freedom of information and academic freedom, there is a point when even halting tentative steps in a direction that leads into conflict with that absolute value must be described in those terms. For us to say to you, "Wait a minute, it looks like you're taking the first steps in a direction that could lead us into some real trouble down the road."

Now, you felt like there was an overreaction to your suggestions. I feel like your last comment was an overreaction to my response.

Admiral INMAN. It may well be, Mr. Gore. Just as I have reflected back on my comments before the AAAS, I have only one part I would have changed, and that was the use of the phrase "tidal wave." I don't expect a tidal wave as I reflect on it. I expect some pretty choppy waters, however, before we——

Mr. GORE. Well, I think you're on an isthmus and there's a tidal wave that could come from either direction. [Laughter.]

Admiral INMAN. Let me ask you a direct question, sir, if I may.

Mr. GORE. Well, that's not the normal procedure, Admiral Inman, but out of my great personal respect for you, I will waive the normal procedure and invite you to proceed, however.

Admiral INMAN. I'm grateful.

The point really is, would my concerns that I express as a knowledgeable, personal viewpoint, have the same concerns if I spoke them as a private citizen, out of office, as they do when I come forward as the Deputy Director of Central Intelligence. Because this is a topic on which I feel so strongly, that the country needs to pay attention and needs to be concerned, that I have to make some decisions about how one can ultimately contribute best.

If whenever I raise the concerns I'm going to find it treated, at least in the media, as somehow the intelligence agencies trying to throw a net over the public, then I can't usefully contribute to the dialog.

Mr. GORE. I think the answer to your question is quite clearly, yes. There is a changed perception of your remarks because you are in the position that you hold, and because they come at a time when the new administration has taken other steps which, to some observers, make up a pattern that is troubling to them.

Let me ask just two final questions lest I encroach on my colleagues time.

First, I guess more than a question, less than a question, is simply a statement that I referred to during your opening remarks. I have carefully reviewed the evidence, and I asked the intelligence community, both at your shop and elsewhere, to describe in detail what is it that has come from the academic community, from the research community, that has given rise to this degree of concern.

Now, I am perfectly prepared to believe that it is difficult to gather such evidence, and that it is difficult to present it in a way that engenders in others the concern that you feel. But I have not been convinced that the degree of leakage or hemorrhaging from the academic community is such that it would override the concerns about taking even halting steps under the goading of someone in a Government national security position post.

I wonder if you want to address that.

Admiral INMAN. Mr. Chairman, the study which will come forward to you, which you will include in the record, does at least have some specifics in a couple of areas. We have broken out some hard data on the targets, on the particular areas in which we know the Soviets are concentrating their efforts and will concentrate them in the months and years ahead.

A good deal of the basic work in these areas is being done on campuses, in research centers. Not in all campuses, only those where they have agreed to work specifically with the Department of Defense or other entities.

You will recall in my remarks that I focused at this point in time that I believe the actual outflow of value to the Soviets from the academic sector is a very small portion of the overall problem.

Mr. GORE. Yes.

Admiral INMAN. If we are increasingly successful in the counterespionage activities against the large leakage, I think the academic community is likely to find themselves a substantially greater target than they are now. I believe these areas will help to some substantial degree refine at least where the first interest ought to be placed.

Mr. GORE. Very good. One final question now.

In order to put your concerns and your statement in the proper context, is it fair to summarize what you're saying as follows, or what you would like to be perceived as saying, that as a private citizen, who happens to have familiarity with the flow of information and technology to the Eastern bloc, you would like to see greater sensitivity within the academic and scientific community in this country, and some thought given to that concern on their part. But, neither as a private citizen nor as a responsible official in the national security apparatus, the CIA, are you contemplating or preparing any sort of follow-on initiative by the Government to attempt to enforce such activity in the academic community if they do not, on their own, recognize such an obligation?

Admiral INMAN. That's a fair and articulate capsulization of my views. It is precisely the latter part of that, based on knowledge of Soviet successes, that led me to worry about what other branches of the Government might ultimately propose in the way of regulation.

The intelligence community will have essentially no role in writing the regulations. We will put forth what we see as the danger, as the leakage. Any regulations would come from other parts of the executive branch.

Mr. GORE. Well——

Admiral INMAN. And in consultation with the Congress.

Mr. GORE. I was giving you a chance to allay my concern, but——

Admiral INMAN. I really didn't intend to allay your concern, nor that of the scientists. In this case I'm saying that I think 6 months, a year, 18 months down the road, as the full magnitude of the Soviet's success of acquiring technology in the West comes to the front of the agenda to be considered by the Government, and the Government decides how to react, at that point I believe there will be proposals to try to regulate it.

Mr. GORE. Are you talking about Mr. Brady?

Admiral INMAN. I think it may come from a combination of Commerce, Defense, State, the entire national security apparatus. And at that point in time it would be very helpful if the academic world had given some very serious consideration themselves to both the depths of the problems and suggestions on how to deal with it.

I may be wrong. The country may decide not to deal with the problem at all and let the outflow continue. I think it is more likely that we will ultimately come as a government to decide to take some further efforts against that outflow.

Mr. GORE. I will have to pursue this at another time. I think you ended up—maybe not you personally, but you ended up placing the Government on the other side of that line, because I don't think that threat is one—and I don't mean to characterize what you said as a threat—but the threat that you perceive, that you say you perceive, I don't think that that's going to be——

Admiral INMAN. I should not endeavor to speak for my colleagues. They're the ones who will come to the role ultimately of where they believe some further measures to impede the hemorrhaging are necessary.

Mr. GORE. Thank you, Admiral.

Mr. WALGREN. Thank you, Mr. Gore.

The Chair recognizes Congressman Brown.

Mr. BROWN. Gentlemen, I appreciate the statements you have made this morning. Obviously, this is a very sensitive area in which we have over a number of years been trying to achieve a delicate balance, and that is always something that is subject to change. I don't think it is unusual to expect that this administration would want to review that balance when it comes in, nor should it be surprising that those who are disturbed by that effort sometimes engage in some fairly strong rhetoric about the fears that they have with regard to disturbing that balance.

I have a concern about the balance in many ways, but I hope that I can give you credit for seeking a rational effort to establish a better balance rather than to destroy the foundations of American freedom or whatever it is you may be accused of doing.

In order to improve the results of this hearing, I would be grateful, Admiral Inman, if you could provide the committee, as you have indicated you would, with that list of technologies which you feel have leaked to the U.S.S.R. I would suggest, if you don't mind, that you do your best to enhance the classified version, which I gather is in the hands of the Select Committee on Intelligence, that some of us might want to look at both in order to determine just what the situation is.

This leads us to my next question. Who makes the decisions as to whether this drain of technology is a serious threat to American security, or damaging to the American national interest, which is a term that you used? I am sure it is no secret to you that Congressmen are notoriously different and they span the entire range of views. We all have deep respect for each other, but very rarely do we depend upon another Congressman to make our views for us.

Now, the question is, Should we turn over to you, or to somebody in the administration, the prerogative of establishing what our views will be on what is the national interest, or even what is national security?

I would like to have you elaborate on how you think the Congress should properly be involved in making these rather fundamental decisions of policy with regard to what constitutes the national interest and the national security?

Admiral INMAN. If the process works as I think it should, Congressman Brown, we will eventually reach the point where the administration examines the current mechanisms by which one manages the flow of technology from the country, the international transfer and arms regulations of the State Department, export controls as they apply, and the Defense Department role as well.

The Congress has a number of avenues available to it to influence that discussion, even in the executive branch, as it is ongoing, probably no way more forcefully as you demonstrate so often in the appropriations and authorization process for the various departments.

My own perception is that ultimately we will reach the point of legislation that deals with how this mechanism interrelates among the departments, that there will be a review of the state of the legislation. It may be that that review will, in fact, not ever really address the part that I'm talking about here, that we will ultimately reach the decision that we will put our efforts on the 70-percent

rough estimate of an outflow based directly on military technology and not on the underlying independent science and research. If that's the case, then we will not end up—unless Congress takes the initiative—in addressing that final sector.

But I believe the process will work to the point that you will have serious proposals to consider a year or year and a half down the way. Whether you should wait for that, or whether you should start your own initiatives, I think I would probably not be brazen enough to suggest to you at this point in time. Though I do think the flow of information, getting people to seriously address the problems, and starting a debate—not a debate, but a discussion—on what values have accrued to the United States through the exchanges. I know of some values. I know simply in the process of ultimately being able to hire analysts in the intelligence community who understand Eastern Europe, that some benefit accrues under the IREX process, of students who study there for some extended length of time.

In my own personal approach to the problem, I would rather not lose that as part of the overall effort, but I think we do need to get the debate off of the flash words of either a tidal wave on one side or academic freedom on the other, and understand the benefits back and forth. I think Congress does have the potential for helping move that along faster than the administration otherwise is likely to do so.

Mr. BROWN. Well, you're going to have a problem, as we in Congress have found many times, in outliving your statement about the tidal wave. I see the April issue of Technology Review again quotes your statement, in which you say—this is the one you made in January, I guess—that it is thoroughly documented that the bulk of the new technology that the Soviets have employed in their military buildup has been acquired from the United States. You describe this as a hemorrhaging of this country's technology and you anticipate a tidal wave of public outrage.

Admiral INMAN. The only part of that that is left for question is whether or not the tidal wave is going to come. The other is documentable fact.

Mr. BROWN. Well, I have asked you to submit that documentation for the record, as you have indicated you would.

Let me ask, Mr. Brady, if you recognize this statement. It says here that "While technical data of conceivable adverse significance to U.S. national security and foreign policy are, on occasion, publicly available, the impact of their availability on the U.S. national security or foreign policy is likely to be minor." Then it goes on to explain the reasons for this. This is a 1979 report of the Department of Commerce.

I presume you don't agree with it, and I wouldn't necessarily expect you to, but I would suggest that you read it so you can thoroughly understand why you differ from the conclusion made by——

Secretary BRADY. Mr. Brown, let me make a couple of points.

One, in the 5 years—I believe that's a 1977 report—there has been a tremendous amount of information developed in the executive branch, certainly in the intelligence agencies, and this process began, as a matter of fact, under Dr. Brzezinski in the last year or so of his tenture at the National Security Council.

Second, I don't think it's a secret to some of the members of the subcommittee that in 1978 and 1979, as I was deputy director of the office that submitted that report, I differed in substantial terms before the House Armed Services Committee about some of the statements that were being made by representatives of the executive branch to the Congress. So I would have absolutely no problem in disagreeing with those conclusions. I think in point of fact, however, that the basis of what we learned in those 5 years is significant.

Just one last comment. A question was raised as to what real impact the academic and scientific community has on the transfer and how important is that impact. I would only make the point that what we have learned in the last few years is that the acquisition of technology by the Soviets is a well-coordinated, integrated entire approach. In other words, they buy what they can; what they can't get, they'll steal. And if they have problems meshing the two, then they get the information through a different way. That's why the exchanges are important and that's why the student exchanges are important.

So each and every part may have little relevance to the whole, but as the whole, it is tremendously important.

Mr. BROWN. Mr. Brady, I would appreciate it if you would expand in writing later on your reasons for the change in conclusions. But I would point out that what you have described is exactly what China, Japan, and most other countries do who face a competitive disadvantage in technology with the United States. They proceed to acquire it as quickly as possible, through every means available, and that includes exchanges of all sorts, occasional industrial espionage or whatever they need to do. I understand that some of our closest allies like France and Canada may do the same thing. For you to imply that there is something unusual about a country like Russia doing it I think is erroneous.

There is one additional thing that I would very much like to have all three of you gentlemen do for the record. I am sure you know that after your testimony we have some distinguished witnesses who will present other and possibly even different points of view from yours. I would appreciate it if in due course you could review their testimony and comment on it for the record so that we might have a rebuttal process and enlarge the dialog to that extent.

Would that be agreeable? I think it would be very helpful to us.

Secretary BRADY. We would be pleased to. (See appendix, Executive Branch Comments on Testimony of Public Witnesses, p. 175–177.)

Mr. BROWN. Now, let me ask one additional question, if I have some time to do so.

Admiral Inman, in suggesting areas of technology which you thought might require some additional controls—you mentioned several and I'm going to ask you about one. You have also, I think, made the point that there are areas of technology in which the item itself may not be sensitive or related to the national defense, but it leads to other areas which might be.

I want to ask you specifically, since you mentioned agricultural crop forecasting, whether our concern is with the Russians having information about our projections of global production for the

97-341 O - 82 - 4

forthcoming year, or whether you are mainly concerned about the Earth resource observation technologies which lead to our ability to do that.

Admiral INMAN. The concern, Mr. Brown, lays with evidence of Soviet manipulation of the market, and of concern that the availability of crop projections facilitated that. One may end up accepting that this is an area that we simply cannot deal with, but what I was trying to get across in those remarks is the breadth of information which they scoop up and put to use. And it was in the manipulation of the market.

Mr. BROWN. I think that is a very legitimate concern. I think it is obvious that the Russians have manipulated the market, to our great disadvantage, and we need to do something about it. But I honestly believe that you would have been doing your own cause a greater service if you had elaborated on that aspect of it instead of just making a statement that we ought to put restrictions on the availability of good crop forecasting. There is nothing the American farmers need more than good global crop forecasting.

Admiral INMAN. Again, Mr. Brown, I hope you will read the Science News coverage, which I put in, which is vastly different than the bulk of the rest of the coverage.

Mr. BROWN. But, you see, this illustrates a particular policy point. The fact is that we do need to do something about the Russian's capabilities to manipulate our markets, or any other centrally dominated State. As a matter of fact, some of our allies do that also, where they can.

The real policy question is how does the United States respond to that—by concealing information or by taking policy steps necessary to redress that. What I'm interested in is the process by which the Congress can act intelligently to take action most helpful to the public welfare of this country.

It is my opinion that when you move the balance too far one way toward concealing information, or restricting the flow of information—I don't want to use a pejorative term—that you may inhibit the capability to make the sound policy decisions necessary to react adequately in the situation.

Would you care to comment on that?

Admiral INMAN. There is clearly a balance to be struck. We tried with Congress to establish in this last half of the seventies a mechanism which will make it possible for you to see classified information which guides the administration in its deliberations, by the creation of two select committees, by depositing information there, by having it available to all the Members to review. I realize that has not proven satisfactory to many simply because of the pressures of time and since they can't rely on staffs to do it as they do otherwise. I frankly don't have a better idea at this point in time on how to make available the classified information.

I don't think declassifying the evidence, on balance, is the right way to go, because in an open society it is extraordinarily difficult to classify information. But in a closed society, they find it very easy to do, and they find it very easy to pin down how we are discovering what they are doing and to go cut off the faucets.

Mr. BROWN. Admiral, I am sure you know that you and I have some differences with regard to the classification of information,

and I won't belabor those, but I do want to raise again the question of how you resolve them and who makes the policy decisions.

Do you think the Congress has a role in that?

Admiral INMAN. We operate now in some of these areas, Mr. Brown, under Executive Order. We operate under those in things like the organization of the intelligence community, because several administrations have ultimately decided they did not want laws, and the Congress has proven reluctant to pass laws.

It will be no great surprise to some members here that I lobbied hard for legislation on the intelligence community, to structure how it would be organized, how it would be run. But as perhaps with this lance that I'm carrying in this current situation, there was not an appetite to undertake that in either the legislative or executive branches.

If Inman, as a private citizen, may express his view, I think getting on to legislation as opposed to Executive Orders is, over the long balance, a preferred approach.

Mr. BROWN. Well, the intelligence area is not the only area in which most administrations take the view that they prefer not to have Congress meddling in their business. Ultimately, as you say, we have tools with which to redress those attitudes, but whether we use them or not is——

Admiral INMAN. They tend to be rather effective when you use them.

Mr. BROWN. Yes.

Thank you, Mr. Chairman.

Mr. GORE [presiding]. Mr. Walgren.

Mr. WALGREN. Thank you, Mr. Chairman.

I would like to explore this hemorrhage you refer to, Admiral Inman. Would I be right in concluding that you're breaking this down into two categories of information transfer? Seventy percent being sort of government-to-government or Defense Department to Defense Department—strictly military, the kinds of transfers that we have already focused on to restrict—with apparently limited success. And then you have the other 30 percent, where there is some benefit of transfer, a very small percentage of which is research and university related?

Admiral INMAN. That's not quite what I was trying to convey, but I don't have any basic disagreement with the ultimate conclusion you get to.

Mr. WALGREN. What I'm sort of trying to ascertain is your agreement that there has not been significant harm in this area yet.

Admiral INMAN. There has been some harm, and there are even some examples where it's significant. It is not, relatively speaking, compared to the other losses, a large part of the problem. It is clearly the area we have been very slow in addressing, the counterespionage side, and that largely has to do with resources applied to the problem, resources available to the FBI.

Mr. WALGREN. You wouldn't use the word hemorrhage to describe that sort of transfer?

Admiral INMAN. I would use hemorrhage as to the outflow of what the Soviets have acquired, and by a wide range of means. Overwhelmingly, the most successful of those means has been the espionage efforts, but some of that has been totally open. We are

such an open society that they can get huge volumes of data and then very specifically target for the pieces which are the immediate payoff.

Mr. WALGREN. But in response to Mr. Brown's asking for documentation of the word "hemorrhage," you're really focusing on the whole range of the transfer, 70 percent being in these areas we have attempted to control in the past——

Admiral INMAN. Precisely.

Mr. WALGREN [continuing]. And a very small percentage, even of the remaining 30 percent, being in the area of university and basic science research.

Admiral INMAN. That's correct. And I am also leaving, Mr. Walgren, in the hopes that we are going to be more successful as a government and with our allies, in stemming the high technology, the direct application, where they get the design of a warhead system or the design of a missile guidance system, and that as we are successful in closing those, we know from other areas the attention then will increasingly go to the areas that are uncovered. What does one do then?

Mr. WALGREN. Just to make the point again that the losses in this area, in your view, are not yet significant—that is how you described those losses in your submission for the record from the Science News publication. You said, "I believe it is necessary before significant harm does occur." I would take from that, at this point anyway, in that area you do not see significant harm as having occurred. So whatever the hemorrhage is that you're going to document for Mr. Brown is probably going to come by and large in that other range, certainly at this point.

Admiral INMAN. The point I tried to make in response to Chairman Gore earlier, Mr. Walgren, was that we know where they're focusing their interest. We know the problems that are out ahead. The effort here is to focus attention on that area and see what can one do to impede it.

You will never control it without unacceptable damage to the U.S.A., so you're not talking about how you get a hundred-percent shutoff.

Mr. WALGREN. I wanted to just ask a little bit about the premise that, as they are cut off—and apparently you're assuming that you will be more and more effective with respect to the area in which the hemorrhage has already occurred——

Admiral INMAN. Hopefully.

Mr. WALGREN. Assuming you are more effective, they will apparently divert their attention to this smaller portion of our concerns.

That really implies that they have not focused much attention in basic research areas as of yet.

Admiral INMAN. You will note in the Science News reporting of my statements at the time that I believe the primary problem at this point was in applied sciences, and that there had been very little impact on the basic research. I said then that it was in applied research where the overwhelming percentage of benefit had been obtained by the Soviets.

Mr. WALGREN. But I get from your testimony that nothing significant has happened thus far, or at least that's the exact word

you used, and you anticipate a greater shifting of focus onto the universities and the basic research.

Then my question is, Is it really true that they have not focused their efforts on the universities and the basic research areas of our society in the past?

Admiral INMAN. The heart of the evidence available to us would show that they have screened information across the whole range, anything that's available relating to present and future U.S. progress in science and technology. But the heart of the efforts have been on applications, things that they can use in the very near term to get into production, cutting short substantially the amount of time necessary to get into production of systems.

Mr. WALGREN. With respect to application and the general approach to what we retain—and I gather we're talking here mostly about manufacturing processes—would you excuse the nonapplied side from great apprehension that there's going to be a transfer which would justify draconian measures that might chill the flow of information?

Admiral INMAN. I have never presumed that draconian measures against the basic research side were either warranted or likely to occur.

Mr. WALGREN. Is it true, too, that when a manufacturing method becomes generally available in the world, if it can be procured from Italy and France and other areas, then we would no longer have a true interest in preventing discussion of that?

Admiral INMAN. We will certainly have lost the ability to control the transfer. It is the advent of multinational corporations, the advent of great growth in research and development activities in Western Europe and Japan, that makes this a very complex problem to deal with. It is by no means a technology loss only from the United States. It is from all across the West.

I think if you will look at the registration of patents in this country, as I understand it, an increasing percentage of the applications in recent years has come from foreign subsidiaries.

Secretary BRADY. Mr. Walgren, may I insert a note?

You mentioned that when it becomes available in France or Italy or whatever, that we cease to achieve an element of control. That is not entirely accurate because that's why the COCOM system, the multilateral system of controls, exist. That's why we maintain them with our NATO allies in Japan. We do, and I think we have achieved, to the extent we're willing to be firm about it, a degree of control to our potential adversaries of the kind of technology and equipment that would be available in other countries.

This administration has embarked, as a result of the President's commitment in Ottawa, on redesigning that system of multilateral controls.

Mr. WALGREN. We speak of some kind of gathering government initiative in this area 18 months down the road and the like. What is the degree of coordination and development of that response? Can we be satisfied that the proper people in the administration are, in fact, talking to each other on an ongoing basis so that perspectives from various concerns will be considered and incorporated into whatever is coming in 18 months?

Dr. MILLBURN. Of course, the responsibility ultimately for the order will not rest with the Department of Defense, but we have submitted our inputs with respect to how we think the classification procedure should be.

Admiral INMAN. I think this goes far beyond just the classification procedures. It really gets to the whole question of how one looks at and coordinates outflow of technology and whether the current mechanisms are working well, if I understood Mr. Walgren's question.

Secretary BRADY. Mr. Walgren, there is no question but that there is an extensive interagency system that I think at this point works fairly well in meshing the views and the information available from me to the agencies so that the final result that is agreed to, either at the Cabinet level or by the President himself, reflects a good consensus of what should be controlled, and the best means to achieve that control.

Mr. WALGREN. Well, let's look at that, then, in one specific case. The President has now apparently decided to withdraw from IIASA.

Was that decision the result of input from all these various agencies that are working on this proposal?

Admiral INMAN. None of us are your expert witness for that decision. Each of us probably had an input in a way on the intelligence community side. We documented the use of the mechanism in some specific espionage activities. A case in Norway comes specifically to mind.

Mr. WALGREN. Let me pursue this for my own purposes, because I am on a committee that looked at U.S. involvement in IIASA. As I understand it, the CIA's concern with IIASA was limited to the fact that somebody associated with the organization used it as a cover, just like somebody associated with any institution, like a university, might use it as a cover to contact somebody in the West and talk about some work that was not related to the institution.

Is that the CIA's reservation, that it was used as a cover? If so, how can that justify withdrawing from an organization, because there are multiple covers out there?

Admiral INMAN. Mr. Chairman, first, there were more concerns than just cover. But again, let me underline that was an input. It is my understanding that wasn't the determining factor at all in the decision not to proceed. Again, I am talking to you from secondhand knowledge.

But my understanding is it was a combination of the National Science Foundation's budgetary constraints, the question of whether the use of funds in IIASA were, in fact, an efficient use of the limited funds that were still going to be available, that the work had not been of the quality or value to merit further expenditure of the funds, and the lack of Soviet reciprocity, where they didn't provide access to a single Soviet data base, whereas the Soviets got access to a wide range of Western data bases, these all were factors that have impacted on the decision which has been made.

I can only report those. I can't speak with direct knowledge on any of them.

Mr. WALGREN. I have used the other Members' time and I apologize.

You know, I am the first one to take a cautious approach toward national security. What concerns me is that there apparently is a psychology out there of which your goading seems to be reflective. That psychology is to be extremely apprehensive about what might happen in this area. I believe we have to be apprehensive, but then when it becomes a basis for actions which, if we truly look at them on their merits, are not justified, I'm afraid it really cuts off our nose to spite our face.

I just want to say that I appreciate your underlining your role as simply pointing a direction or goading—which implies driving farther than may be necessary in order that people think about this—and differentiating that from the reality of actual policy decisions. But I am very much afraid that others in the Government will be driven by that fear and take actions which are not in our best national interest because of it.

I realize it's a very difficult area and one where clear lines cannot be drawn. But I appreciate your testimony before the committee and your responses to our questions.

Thank you, Mr. Chairman.

Mr. GORE. I take it that you share that last concern as well, if I understand your testimony.

The Chair will continue to recognize my colleagues in the order in which 'hey arrived, according to the rules.

Mr. Shamansky.

Mr. SHAMANSKY. Thank you, Mr. Chairman, Admiral, and the other gentlemen on the panel.

In 1960 I traveled to the Soviet Union as a tourist, and in the Metropol Hotel in Moscow I asked the Intourist Office if I could have a map of the underground. They said they only had one in French. I said I could handle that, so they gave me one. An Englishman right after me asked for one, and they said they didn't have any, suddenly.

It was a vivid illustration for me, that in any kind of society in which there is a premium on not taking responsibility for making a mistake—and the Soviet Union, it seems to me, is a classic example of that kind of society—it is always better to say no. Then you can't be blamed.

Now, with respect to the ability of the administration to make important decisions, we, on this committee, have tried at least to get rid of the Clinch River breeder reactor at about a quarter of a billion dollars a year, but the administration, in its infinite wisdom, keeps putting it back, even though Mr. Stockman said in 1977 we shouldn't have it at all.

I bring that up to say a faith in the ability of any administration to make great decisions is a little worrisome to at least this member, who is in real life a lawyer and while in the Army was trained as a counterintelligence corps special agent. So it isn't just a question of academic freedom for me, at least. It's a question of really the basic first amendment freedom. I am not anxious to turn our open society, as you keep referring to it, into a closed society, because they do something better in the way of being a closed society. I think that is true, and more power to "them" in that terrible goal.

It seems to me that if one thing we have learned, at least I have learned in this past year, that science and technology in the international sense is really fungible. The Japanese didn't make all this technology that they have been applying. It originated here. They applied it better. So to keep the basic information back I think is chasing a will-o'-the-wisp, some kind of a chimera, that you're pursuing.

I find it an almost pathetic confidence in the ability of Government to control knowledge, when this administration has so little faith in the ability of the Government to do anything else correctly.

I have great difficulty imagining our—you say we're not going to touch the basic research stuff, it's just the application. But that's pretty far down the road, isn't it?

Admiral INMAN. Mr. Shamansky, with all great respect, I don't think you have really heard—you did come late, admittedly.

Mr. SHAMANSKY. Well, I did try to read this, if it's at all a fair summary, and I apologize. I just got off the plane and came straight here.

Admiral INMAN. I have not put a proposal on the table to control anything, so any illusion to that or any reflection back to reporting in the major news media that reflects that is flatly erroneous.

What I have said, and what I continue to pursue, is that there is an enormous outflow, not to a friend, but to an adversary, and to an adversary which has used it to enormous advantage in building military force, shortening the research and development time to get the weapon systems greatly because of their ability to draw on that resource.

There is nothing that says that is going to slacken at all. None of the initiatives that we're doing appears thus far to be impacting on the pace of that Soviet buildup. One then must turn to look at the outflow which sustained that, to say are there ways in which you can impact positively in halting that flow.

There clearly is a large measure of that outflow that is successful through espionage activities and getting hands on designs, on buying, legally and illegally, microelectronics.

There is some, much smaller, focus on research being undertaken in research centers and academic institutions. I don't accept as a premise that one can never consider constraints on public flow of information in that area, because those centers are already expert at limiting that flow when they're doing it under contract for industry for proprietary purposes, and increasing numbers of them are examining how to do that when they want to acquire patents to help pay some of the increased costs of education. So my efforts to this point, and continually, are to draw out of that same talent what are ways one could potentially impact on the flow out to the Soviets without being any greater a threat to academic freedom than has been that which they have already devised and accepted in dealing with industry and in dealing with their own prospects for getting patents.

Mr. SHAMANSKY. I try very hard not to use the word "existential" because I'm not quite sure what it means all the time. But it seems to me that this is an existential problem in our kind of soci-

ety using this kind of information; namely, it's implicit, it's inherent in the situation. It seems to me——

Admiral INMAN. Mr. Shamansky, that was exactly what I was told when the cryptology issue came up. In fact, there the academic world came up with ideas, ideas which were not, in fact, those put forth by the government at all, but they appear to be working and working effectively.

Mr. SHAMANSKY. But is there anything now that would prevent—in other words, my approach right now is "If it ain't broke, don't fix it." If you're working these things out—and you're giving us shining examples of the success of what you're advocating—there is nothing in the law now that would prevent a repetition of that.

Admiral INMAN. Not at all. And the whole purpose of my dialog from the outset has been, rather than—you needed to have been present at the AAAS to have gotten the full flavor of the scientists who were present, in large measure saying "no regulation, no restriction of flow under any circumstances can ever be considered."

Mr. SHAMANSKY. Then basically, I gather, you're sort of reporting on what is going on and not really asking for further legislation?

Admiral INMAN. I'm not at all asking for further legislation. I think the prospect may come down the road where legislation may be contemplated, and I am trying to play—not very successfully, obviously—the role of gadfly to get my academic colleagues to start thinking about what they can do.

We talked about legislation, Mr. Shamansky, on the cryptology issue. The academicians objected to the idea of going to legislation absolutely, and then thought they could find other ways that would meet the Government's concerns. In my view, they were successful. I am looking for that same kind of wisdom to deal with a larger issue of technology transfer.

Mr. SHAMANSKY. Well, I realize it is one of the fallacies to argue by analogy, but I think of knowledge in the science and technology field as fungible. In other words, what we know here would they know in France and England and even in Argentina, and I say Argentina because we tried to have a grain embargo against the Soviets and our friends, the Argentines, sold the Soviets all the grain, you know, getting around that.

So what is to prevent our allies from exercising their ability—I realize you said we have CoCom, but there are other technologically advanced nations which are working on things and we may not know if it's a friendly country and we'll export it there and then they'll have the industrial espionage in those place.

Admiral INMAN. They are also targets, Mr. Shamansky, for certain.

Mr. SHAMANSKY. Yes, and that's my point.

Admiral INMAN. And we have some dialog with them, sharing knowledge. I don't know to what degree any of them are going to address at this point in trying to deal with the problem. I do know that at least the more advanced ones share some concern about the degree to which the outflow has taken place. Whether that is going to transfer into any actions is an entirely different question.

Of course, in some of those countries there is substantial government ownership which puts them in a different manner in which

to deal with the large problem, but that is still—My understanding, particularly from the Chairman, of the primary concern here was that we were going to rush pell mell off to develop legislation to somehow restrict or impede academic research in this country.

Mr. SHAMANSKY. Speaking of academic research, sir, one of the reasons I am on this committee and wanted to be is because in my home community we have Ohio State University and Battelle Memorial Institute, and Chemical Abstracts, among others. I think that the future of not just my home community but this country rests in the continued effective cross-fertilization of knowledge in just this area. I am very sensitive to this, not just because of my political capacity, but my training as a lawyer and political science, in really resisting any unfortunate attitude on the part of any person in Government who would rather not give out the map to the subway in Moscow because it is always easier to say no. You can't be blamed then.

That's a real problem. I mean, I don't think this is just some high-flying principle. I think it works badly at all levels of government, and I think it behooves us to be very cautious about changing that balance.

Thank you, Mr. Chairman.

Mr. GORE. Mr. Gregg.

Mr. GREGG. Thank you, Mr. Chairman. I won't use the term "existential" because I don't know what it means. I won't even try. [Laughter.] I won't even mention Clinch River, in deference to our chairman. [Laughter.]

Mr. GORE. I was hoping that was the royal "we" and not the collective "we."

Go ahead.

Mr. GREGG. I would like to make a statement first. I think maybe I'm a little more sensitive to this because I'm lucky enough to come from the State that lent Washington Larry Brady, who has made us in New Hampshire a great deal more sensitive because of his background in this area, to what I consider the legitimate concerns of Commerce, CIA, and other Federal agencies in the so-called hemorrhage. Whether it is a hemorrhage or not doesn't really matter. Even if it's just a slow leak, as far as I'm concerned, the delivery of high technology, military applicable information and materials to the Soviet Union is not good for the United States in its own self defense. That is why I am so pleased to be sitting here today to hear Mr. Brady's testimony.

I will say this, I think there have been some representations on the other side here that reflect the fact that there is some sort of absolute right to an interchange of international knowledge and that the Soviets should have an absolute right of entry into our scientific community just because we have a free society.

Well, as we know under our Constitution, our free society, for example, allows travel and absolute right of travel within the United States. But as the *Agee* case showed us specifically, that right of travel is qualified when you get beyond the State borders.

Clearly we have an absolute obligation for free exchange of information within the United States, but when you're dealing in foreign policy and you're dealing with a nation which has invaded Afghanistan and crushed the Polish people, I think you have got to

take a little more tentative position when you start delivering to them information which they can then turn into weapons and use against peoples of the world.

I think the people testifying today, especially the admiral, have made it clear that they're not planning immediate regulatory activity, and I commend them for that because I will have to agree with Mr. Shamansky that the Government doesn't seem to do too many things right, and maybe there is an inconsistency in asking the Government to participate in this area.

But what I would like to ask the admiral, and what I would like to ask Mr. Brady, is how can we initiate greater incentive in the private sector to participate in this effort to limit the outflow of information which has occurred? How can we encourage the cryptologist situation and other activities?

I would like to have Mr. Brady answer, and then the admiral.

Secretary BRADY. Mr. Gregg, first I think it is useful to disestablish, as I think you have done, some of the myths surrounding this question. We cannot envelope every research activity in academic freedom. As my statement tried to point out, it is some of the new activities of research institutes, particularly associated with universities, in getting into the applied area and industrial processes area that are causing the problem.

So that what we are trying to do is to work very closely with the scientific community—and we have done that in the last few months. As a matter of fact, as the matter now stands, there are a couple of individuals in the research and scientific community where it is incumbent upon them to come to us with another meeting.

We have taken a look at our regulations. There has been an immense amount of work done by the Department of Defense, the Department of Commerce, and other agencies of this Government, to arrive at what we call a Military Critical Technologies List, and in point of fact, if the Government does anything by way of regulatory activity, it is going to be narrowing, in a sense, the concern to specifically address technologies that we view as immense concern, and then, of course, to bring about a better information base, to education the business and scientific community, the academic community, to a greater extent than before, as to precisely what the regulations are, what we are trying to accomplish, and specifically narrow the focus to the technologies of——

Mr. GREGG. Does that also include educating the community as to what you perceive the Soviets are after?

Secretary BRADY. Absolutely. Admiral Inman indicated that they are working on a declassified version of what this technology transfer effort by the Soviets has accomplished. If that can be published, I think we will make great headway in that public education campaign.

Admiral INMAN. Mr. Gregg, for all of the bad things that flowed out from my perspective, of the coverage of my January foray into this effort, there were some things that I have been happy about. That is getting on with addressing the problem in some of the private sector areas, for which they have been kind enough to say they were spurred to do so out of that speech.

I think some of your later witnesses today will describe in some greater detail. The most encouraging efforts from my point of view are the ones that have come under the National Academy of Science and National Academy of Engineering, where they have sponsored getting on with a review—the National Academy of Sciences, I believe, is sponsoring a review of scientific communications and national security, with a report to be finished late this year. Essentially, they are playing the honest broker role that the American Council on Education played earlier in addressing the cryptology issue. So I think that is one to watch, to support, and not to intrude on, but it may well at least give us the next leg up in getting to address the issues, as opposed to just the atmospherics surrounding the problem.

Mr. GREGG. Thank you.

I would suggest also, and I think you have hit a bit of a key there in mentioning that the effect of your statement was just the fact that you made the statement. I believe the awareness level in this country has lifted dramatically over the last year on this entire issue, thanks to your efforts, thanks to Mr. Brady's efforts, and thanks to Mr. Millburn's efforts. That, in and of itself, is very important.

I think the average retailer or wholesaler of American knowledge and goods wants to be sensitive to this issue and is willing to take action to be sensitive to this issue. They just weren't aware of it. I think if nothing else you have contributed greatly in that area.

Admiral INMAN. Thank you very much.

Mr. GORE. Admiral Inman, you referred to the value of continued exchanges. Of course, exchanges are only one aspect of the subject under discussion.

I wanted to ask Dr. Millburn, since it has been suggested by Mr. Carlucci, among others, that scientific exchanges with the Soviets are one-sided, either because the Soviets are not as technologically advanced as the United States, or that the Soviets have not been forthcoming in making that technology available to U.S. scientists.

Do you believe that scientific exchanges with Eastern bloc countries are mostly one-sided, and if not, what, if anything, is the United States doing by way of exchange and similar programs to obtain such information?

Dr. MILLBURN. The exchange of technical information between us and the Eastern bloc I think is by and large one-sided. We do get minimal benefits back from it, primarily, from my point of view, in our ability to assess where they stand in certain areas of technology. So far as our ability to enhance our own technological position as a result of those exchanges, I think that is very minimal.

Mr. GORE. All right.

At this point let me enter into the record, without objection, the exchange between Frank Carlucci, the Deputy Secretary, and William D. Carey of Science magazine on this subject.

[The information follows:]

[From Science, January 8, 1982, p. 139-141]

SCIENTIFIC EXCHANGES AND U.S. NATIONAL SECURITY

On 9 October 1981, in a letter addressed to the Honorable Frank Carlucci, Deputy Secretary of the Department of Defense, Mr. William D. Carey, Executive Officer and publisher of Science, criticized statements by the Department of Defense concerning

scientific exchanges, conferences, and the unclassified, open scientific literature. Mr. Carey's letter and the reply he received from Mr. Carlucci are printed here verbatim.

I must tell you that the otherwise excellent brochure on *Soviet Military Power* went off the rails badly, in my opinion, in contending (pp. 80–81) that U.S.-sponsored scientific exchanges and scientific communication practices enhance Soviet military power.

I am dismayed to find the Defense Department indicting inter-Academy exchanges, student exchanges, scientific conferences and symposia, and the entire "professional and open literature" as inherently adverse to U.S. military security interests. These normal and well-accepted fora for advancing scientific progress constitute the primary infrastructure of U.S. and worldwide communication in science, and without them the U.S. technology base would go stale very quickly.

The Defense Department should know, by this time, how scientific practice is conducted and how necessary unimpaired communication in science is to advancing the state of the art and improving our own essential capabilities. I find it deplorable to have our Defense Department taking a public and well-advertised stance that exchanges and the open scientific literature constitute still another window of vulnerability and a free asset handed to our principal adversary.

It is also somewhat astonishing to have the Defense Department charging that bilateral U.S.-Soviet scientific and technical exchanges are giveaway channels benefiting Soviet military power. These bilateral exchanges, as you must know, are legitimized by former intergovernmental agreements initiated by President Nixon and continued by his successors. Whether the Defense Department likes them or not, they constitute the present foreign policy of the United States. As to the merits, it is very important to U.S. interests to be well-posted on the quality of Soviet scientific research. The contact we have through the bilaterals has left no doubt as to Soviet excellence in fields that matter to us, including metallurgy, condensed matter physics, theoretical physics, astrophysics, geophysics, and cancer research. Nobody is arguing that the exchanges should involve security-related fields of science. Elsewhere, in fields where both sides are equally good, it is to our country's advantage to pursue the exchanges. The DOD paper shows an extremely disappointing grasp of what the exchanges are all about.

If I seem exercised by the position taken by the Defense Department in *Soviet Military Power* it is because I *am* exercised. In particular, that position strikes in a deadly way at the dependence of scientific progress on open communication and shared information. Our own military power will be diminished, not enhanced, if the wellheads of scientific communication are sealed and new knowledge confined in silos of secrecy and prior restraint.

MR. CARLUCCI'S REPLY

This is in reply to your recent letter in which you state that the Department of Defense (DOD) views the inter-Academy exchanges, student exchanges, scientific conferences and symposia, and the entire professional and open literature as inherently adverse to U.S. military security interests.

Be assured the DOD is well aware of how scientific practice is conducted and fully recognizes the importance of unimpaired scientific communications to the mutual benefit of all parties concerned. In our considered view, however, the exchanges to date, in the main, have not been reciprocal. Rather, it is quite apparent the Soviets exploit scientific exchanges as well as a variety of other means in a highly orchestrated, centrally directed effort aimed at gathering the technical information required to enhance their military posture.

Because of the importance I attach to this complex issue, I want to respond in some detail and thus ask your indulgence. Illustrative examples follow which, at least in part, indicate the basis for our concern.

The energy bilateral agreement began with 14 subtopics. The U.S. promised and delivered the large magnet and magnetohydrodynamics (MHD) channel details as well as a great deal of information on other topics. The Soviets promised but did not deliver data on geothermal energy and energy resources, consumption, production, and forecasting. Consequently, the U.S. Department of Energy has been curtailing its participation. The only topic still active is the one on MDH.

Under the S&T bilateral agreement, the Soviets had been sending large numbers of scientists to the U.S. in the field of chemical catalysis, but the U.S. was gaining virtually nothing in return. Consequently, in 1980 the U.S. terminated the one-sided exchange. It now appears, however, the Soviets will try to use the inter-Academy exchange or other means to acquire the information they deem vital.

Another example of their persistence was demonstrated in the electrometallurgy subtopic of the science and technology bilateral agreement. The Soviets wanted to establish an exchange in the fields of superplasticity and fracture mechanics. A concerned U.S. government scientist succeeded in stopping the exchange in these militarily related topics. However, it was dismaying later to find that the Soviets had acquired the information under the auspices of a new subtopic on corrosion.

One of the provisions common to many of the government-to-government bilateral agreements encourages the establishment of separate agreements between individual companies in the west and entities of the Soviet government, primairly the State Committee for Science and Technology and the Ministry of Power Engineering. These are sometimes referred to as the "Article IV" Agreements and in the case of the U.S. involve a large number of companies that are among the world's leaders in areas in which we know the Soviets to be deficient. The degree of concern with this situation was such that previous policy was altered to the extent that the Export Administration Act of 1979 now requires that companies file notice with the Department of Commerce when such agreements are signed.

We also have evidence that the Soviets are misusing scholarly exchanges. In the area of graduate student and young faculty exchanges, administered by the International Research and Exchange Board (IREX), the U.S. sends young master's and doctoral level students, mostly in humanities, primarily to two universities, Moscow State and Leningrad State. For the most part, the USSR sends senior, experienced, technical people. Almost all possess *Kandidat* degrees; some come from closed military research institutes, and attend any of a hundred or so U.S. universities. In accordance with the openness of our society, Soviet students are granted academic freedom and, with almost automatic government approval, can travel practically at will. Conversely, American students in the Soviet Union are much more isolated and restricted in their travel and professional contacts.

Soviet weakness is not in basic research, which, as you point out is on the whole excellent. Rather their weakiness is in putting technology into production. It is therefore not surprising to us that the scientists the Soviets nominate are often directly involved in applied military research. For example, in 1976–77 S. A. Gubin's course of study involved the technology of fuel-air explosives. Mr. Gubin studied this topic at one of our leading universities under a professor who was a consultant to the U.S. Navy on fuel-air military explosive devices. As a parenthetical comment, one must admire their ability to determine so precisely where to send their "students." Gubin, incidentally, during his stay ordered numerous documents pertaining to fuel-air explosives from the U.S. National Technical Information Service. When he finished his study, he returned to his work in the USSR developing fuel-air explosive weapons.

In the case of K. H. Rozhdestvensky, it was not until several months after his departure that we learned his research paper was concerned with the "wing-in-ground effect" aerodynamic vehicle. This vehicle has significant potential military applications and indeed, the Soviets have been attempting to develop a wing-in-ground effect machine for quite a number of years.

T. K. Bachman, a psychologist, came to study the interface between man and machine. In the opinion of U.S. researchers, this field was directly applicable to the design of heads-up displays which optimize the amount of data presented visually to a military weapon system operator. Bachman attended several very significant conferences on this topic and was able to observe state of the art demonstrations of such work funded by the Department of Defense.

This graduate student/young faculty exchange is such that each year it is recommended that at least one-half the Soviet nominees not be allowed to pursue their desired topic of study at all or that significant modifications be made in their study program. This because the information the Soviets seek is either embargoed by law or militarily sensitive. Hence our concern.

In the senior scholar exchange program also administered by IREX, each side sends a number of scholars for a total of 50 man-months per year. As with the graduate student/young faculty program, the Soviets nominate physical scientists, while the U.S. nominates scholars specializing in the arts, literature and history. Until a few years ago, most Soviets in this program conducted very basic research. No objections were voiced to such courses of study. Currently, practically all the Soviet nominees propose to study in fields having military application. Some examples of proposed research topics in 1981 are:

Properties of adhesive joints of polymers.

Macromolecular materials and composite materials (two nominees).

Preparation of micro-tunnel diodes in gallium arsenide by annealing and/or molecular beam epitaxy.

Theory of computer science and programming methodology.

Thin-film metals in semiconductor technology.

Semiconductor and infrared technology, ion implantation, radiation defect analysis and infrared detector techniques and materials.

Machinability of difficult to machine materials.

Largely as a result of dissident physicist Andrei Sakharov's ill treatment, the U.S. Academy of Sciences imposed a moratorium on joint symposia and other high level contact with the Soviet Academy of Sciences. Nonetheless, individual exchanges are still permitted and the Soviets continue to nominate scientists to study and conduct research in topics that are either embargoed or militarily sensitive. Of 25 scientists nominated by the Soviets during 1980, 11 topics proposed offered a significant potential for loss of critical U.S. technology. There was a somewhat lesser, but nevertheless real, degree of concern over the remaining 14 topics.

With regard to scientific conferences and symposia, the Department of Defense has become increasingly concerned over the type and volume of defense-related information openly provided. As you will undoubtedly recall, the concern has been such that Soviet Bloc scientists were prevented from attending the First International Conference on Bubble Memory Materials and Process Technology, and the Conference on Laser and Electro-optical Systems/Inertial Confinement Fusion early in 1980. This denial was precipitated by the revelation that Hungarian physicist, Gyorgy Zimmer, provided the Soviets the scientific knowledge on magnetic bubble memories gained as a result of his frequent visits to U.S. laboratories. A thorough review then followed which resulted in an official U.S. policy restricting Soviet attendance at U.S. conferences and symposia. This policy was widely publicized in a number of scientific journals.

With regard to professional and open literature, U.S. and western applied and basic research papers are usually quite explicit in explaining their purpose and are published promptly and without censorship. The author's affiliation and the sponsor of the research are almost always provided. This is contrasted with Soviet and other Communist country publications where the purpose and goal are usually not mentioned or deliberately obfuscated. Authors' affiliations frequently are not provided and the sponsor of the research is rarely identified. In addition all articles are subject to censorship.

I would also point out that it is and has been for many years U.S. policy to make available all unclassified government sponsored research to anyone in the world at very nominal cost through the National Technical Information Services (NTIS) of the Department of Commerce. Similar Soviet research holdings are maintained by the All-Union Institute of Scientific and Technical Information (VINITI) which is jointly administered by the State Committee for Science and Technology and the Soviet Academy of Sciences. The NTIS assisted the Soviets in setting up VINITI under the auspices of the bilateral agreement on Science and Technology, yet the holdings of VINITI are not released to anyone outside the Soviet Union.

Other examples abound, but I trust that these will suffice to provide you with the context within which our views were framed. The Department of Defense favors scientific, technical and educational exchanges and the free exchange of ideas in basic and fundamental science. However, since the military posture of this nation relies so heavily on its technical leadership, the Defense Department views with alarm the blatant and persistent attempts. some of which have just been described, to siphon away our militarily related critical technologies. I note this is precisely your point when you state "nobody is arguing that the exchanges should involve security-related fields of science." By the very nature of our open and free society, we recognize that we will never be able to halt fully the flow of militarily critical technology to the Soviet Union. Nevertheless, we believe that it is possible to inhibit this flow without infringing upon legitimate scientific discourse. I hope that this letter has allayed your concerns and look forward to additional views you may wish to offer.

Mr. GORE. I was impressed that two of our witnesses here have referred to the willingness of the academic community to restrict the free flow of information when commercial interests are at stake, and to put restrictions on the flow where exclusive patent rights might be at stake.

To what extent do you see that as a model for future efforts by the Government? Maybe my question is an awkward one, but let me tell you what I'm trying to do.

I have expressed concern in the past, as the Chairman of one of the two subcommittees here, that academic freedom and the free

flow of information was, in fact, jeopardized by many of the arrangements made with private corporations. I am tryng to make the point that when you all express your concern, you look at those agreements and you see, well, they're willing to do it there. And here we have a national security interest at stake. What is the difference?

Do you understand the point I'm making? You can play whatever role you want in enhancing that point.

Admiral INMAN. The point you have made is exactly one that motivated me into playing the role of goad.

Mr. GORE. I started to ask you to what extent did that——

Admiral INMAN. There is clearly a problem. I don't know how the problem is going to be dealt with, and I am not at this point prepared to offer solutions. I don't know enough about the impact on the academic side. What I was out to get before, and on this one, is don't just automatically throw up "academic freedom, we can't discuss anything" as the response, because there clearly are already procedures which have been developed to deal with other problems.

Secretary BRADY. I think, Mr. Chairman, it is important to appreciate the changing nature of the "academic institution", specifically as it concerns the very narrow area that we are concerned about, and that is the applied side to industrial processes—you know, robotics, computers, semiconductors. That's what we are concerned about. It is specific and it's narrow.

Mr. GORE. Well, I hope some light bulbs went off in the AAU and the university community due to that response. I certainly think that they should be concerned about academic freedom in the other area as well, more so than I think they have been.

Mr. Brown, did you want to——

Mr. BROWN. May I just ask one or two additional questions?

Mr. GORE. Sure.

Mr. BROWN. Gentlemen, I have tried to review this report of the Defense Science Board Task Force, which I think is well done from my cursory review. I want to ask possibly Dr. Millburn if he has any thoughts with regard to some of the recommendations here. I am looking at the principal findings where it says:

> Where export control regulations continue to pose a problem for the university researcher, DOD can alleviate this problem by negotiating mutually acceptable sets of guidelines for the dissemination of research information, and publication of a new unclassified version of the Military Critical Technologies List would aid in this process.

Would you care to comment as to whether that's a desirable direction to go in from your standpoint?

Dr. MILLBURN. Yes, indeed, it is, Mr. Brown. We are now working very closely with the university community to attempt to devise acceptable guidelines. We are addressing also the problem of achieving an unclassified version of the military critical technologies list. That may be much more difficult to achieve.

Mr. BROWN. Well, I think it would probably help a little to declassify some of that information to offset the perception, at least, that you're overly classifying things over there.

There is another part of this recommendation that illustrates a point that I made with Admiral Inman. It says, "The large percent-

age of foreign nationals in graduate engineering programs is due in part to the decline of the number of U.S. citizens entering graduate schools—". Of course, this is undesirable from a security standpoint.

There are two ways to approach this. One is to start screening foreign nationals and keep them down as low as possible, and the other thing, which I think is much more necessary, is to do something to improve the number of American nationals engaged in graduate training and engineering and science.

The problem with the negative approach to this is that it overlooks the positive policies necessary to really serve the national interest. I brought this point up with Admiral Inman. I think that this may be a part of the general concern of many of us in the Congress as well as those in the universities, that in an effort to do something that appears to be negative we are missing the positive policies that need to be put in place in order to really benefit the national welfare.

I don't pose that as a question but as an explanation for some of the deep concerns that arise in some areas.

Dr. MILLBURN. I would like to suggest, Mr. Brown, that the Department of Defense has attempted to increase the number of graduate fellowships available to U.S. citizens. For example, now the Navy will have 45 fellowships, $12,000 going to the graduate student, $8,000 to the university, and these will be preferentially given in certain areas of importance to the Navy. The Army will have 25 fellowships with similar stipends and support, and the Air Force will have 40 special assistance fellowships in the same way. So we are attempting to address the problem of correcting the imbalance between the graduate students' income and the income which they could get by going directly to industry.

Mr. BROWN. It is unfair for me to point out that if we're so anxious to copy our enemies, that one of the things they do is subsidize all of their graduate students fully.

Dr. MILLBURN. We like to be selective about the parts of their society that we adopt.

Mr. GORE. Let me thank all of our witnesses.

In closing, I want to clarify just one brief point. When you went to the AAAS, Admiral Inman, you were invited to participate as part of a panel that was set up by the AAAS on this subject; you did not request to come and make this presentation; is that correct?

Admiral INMAN. I was invited to go to that panel when I was still the Director of the National Security Agency, to make the case for the need for secrecy, which no one else was willing to do. I committed that I would go, and I carried out that commitment, even though I had shifted jobs in the timeframe.

I think from a personal point of view, the one principal irritation was that I had prefaced my remarks that morning before the AAAS that I was there in a personal capacity. It was the substantial media coverage later and letters attributing CIA's efforts to do things which was most irritating. In fact, a lot of my CIA colleagues wonder why I'm out playing Don Quixote on this topic, which is one I think needs to be addressed.

97-341 O - 82 - 5

Mr. GORE. Without objection, I think it might be appropriate to also put in the record the other papers that were presented on this same panel, which show that it was the scientific community's initial inquiry into how to treat this subject that led to their decision to invite you. The other papers are quite interesting as well. (See appendix, Papers Presented at Symposium on "Striking a Balance: Scientific Freedom and National Security", 1982 Annual Meeting of the American Association for the Advancement of Science, Washington, D.C., p. 178–263.)

Mr. GORE. I think it is extraordinary that in an open society like ours we have the ability to discuss such a sensitive topic as this one openly with representatives from the executive branch. I think the way the issues were raised has been clarified somewhat. I know concerns remain.

I appreciate all of you coming here today. Mr. Brady, we're delighted to have you, Dr. Millburn, and Admiral Inman, thank you very much.

Admiral INMAN. Thank you, Mr. Chairman.

Mr. GORE. Our next panel consists of Dr. Frank Press, President of the National Academy of Sciences, and Dr. Robert Rosenzweig, vice president for public affairs at Stanford University.

Gentlemen, if you would come and join us at the witness table. Let's begin, Dr. Press, with your statement, and without objection, the prepared remarks of both of our witnesses will be put into the record in full at this point.

We would like to begin with you, Dr. Press. Welcome.

STATEMENTS OF DR. FRANK PRESS, PRESIDENT, NATIONAL ACADEMY OF SCIENCES; AND ROBERT M. ROSENZWEIG, VICE PRESIDENT FOR PUBLIC AFFAIRS, STANFORD UNIVERSITY

Dr. PRESS. Thank you, Chairman Gore.

I was hoping that with Admiral Inman's departure we could turn off the TV lights.

Mr. GORE. I think they may be interested in what you have to say, so without objection, we'll keep it available.

Dr. PRESS. I would like to thank you for the opportunity to discuss with your subcommittee the impact on science and technology of proposed government initiatives for increasing national security restrictions in the exchange of scientific information. I am also pleased to describe for you the cooperative role that is being played by the National Academy of Sciences in addressing these issues, and in seeking an accommodation between government and the scientific research community.

As your committee has recognized, the quest for that accommodation presents difficulties in finding a balance between national security and economic interests, and individual rights, including those rights associated with open scientific communication.

The issues leading to the current controversy are not new, and extend back several years into the previous administration. The intensity of debate has increased, however, as public sensitivity has heightened over growing international military tensions and increasing transfer of American technological knowhow to our foreign industrial competitors.

You have heard already from previous witnesses that notable strides made by the Soviet Union in the military sphere have been largely responsible for increased interest on the part of the Government in preventing the transfer of militarily sensitive products and knowledge to our Nation's potential adversaries. In response to these concerns about the leakage of militarily sensitive information, various executive branch agencies are currently reappraising policies on the transfer of technology to foreign countries. Government officials have expressed concern in particular about foreign access to computer science and mathematics research that bears on cryptology, and to research involving magnetic-bubble memory devices, laser-optics and inertial confinement fusion, and very high speed integrated circuitry [VHSIC].

Public attention has also increasingly been drawn to these matters because of the significant competitive success of major industrial countries—success made possible in many instances by the apparent ease with which other industrial nations can draw upon the results of American R. & D.

Technology transfer can take many forms that go beyond the acquisition of hardware or processes. The collection of data and information in the open literature, person-to-person scientific exchanges, attendance at conferences, symposia, and other open forums, and participation in university research and education, all offer the opportunity for transfer of technological data. These transfer issues pose a dilemma for the Government and the university-based scientific and engineering community—one that both parties and the country generally have a high stake in resolving in a mutually constructive and satisfactory manner; yet one, unhappily, in which recent developments point more toward polarization than consensus. The issue can be stated as follows.

Some Government officials believe that a category of unclassified research results exists whose free and open publication or dissemination, especially to particular foreign nationals, could pose an undue threat to the national interest and, at times, to national security. Accordingly, they think it essential to control foreign access to this information.

On the other hand, most scientists and engineers in academia hold that open communications is absolutely essential for a creative research environment. In their view, restrictions on scientific communication sap the strength and vitality of the educational and research endeavors upon which the Nation's present and future technology base is founded. Moreover, such restrictions are seen as inconsistent with a free society and, in some instances, with basic constitutional rights. Neither would they like to see us forced to emulate the Soviet practice of compartmentalizing and restricting access to knowledge.

Traditional means by which the Government seeks to protect and promote the Nation's security and technological leadership include classification of military and diplomatic secrets, surveillance and controls of foreign visitors through visa and travel restrictions, and export control restrictions outside the military intelligence security classification systems.

Increased controls over the transfer of sensitive technical data can be achieved either by expanding the coverage of the military

and intelligence classification system, through, for example, revision of the Executive Order covering such matters, or by the more rigorous application of export controls.

Expansion of the scope of classified information is highly controversial. I offer for the record a copy of a letter which I recently sent to the President's National Security Adviser on proposed changes in the Executive Order on national security information. This letter highlights the nature of these controversies from the vantage point of the scientific community.

Our major concern is that the proposed expansion of the scope of classified information into peripheral areas could force some scientific research indirectly relating to national security out of most leading universities that will not do classified work, thus denying this important resource to the Defense Department and to the Government as a whole. It would be unfortunate, indeed, if by these steps we discouraged major components of the scientific community from continuing basic research in areas of potential importance to the Nation and to our national security. We should consider how much our security is harmed by denying government access to many of the Nation's most brilliant scientists and engineers who work on university campuses.

It is apparent from the discussions this morning that the issue is not basic scientific research in universities. None of the Government witnesses proposed restrictions in this area. But universities are involved in work on computers, lasers, materials, et cetera and placing such restrictions on this work could result in closing out this valuable resource, thus reducing our technical productivity. This must be balanced against potential damage to the U.S. national security, and that's the issue that we're all trying to wrestle with.

Export controls on the transfer of technical data are equally controversial. Interpretations of export regulations are often broadly cast in ways that members of the academic community believe are unnecessarily restrictive. Technical judgments are made by persons within the Government who are often perceived by scientists as lacking competence in a particular topic or discipline or who are not familiar with the nature of scientific discovery. Government officials, from their perspective, think that members of the academic community are often naive or uninformed about the extent and consequences of technology transfers to other nations. Thus, it is important that we have a balanced and objective assessment of the views of both the Government and the scientific community on these controversies.

Mr. Chairman, the interdependence of government and the research community in advancing science, technology and the national security requires the prevention of a breakdown of mutual confidence. In February of this year, I communicated my concerns on these issues to the Under Secretary of Defense for Research and Engineering when I sought the cooperation of the Department of Defense in a study to be initiated by the National Academy on the impact upon scientific communication of government regulations concerning technology transfer. I have also discussed this matter with other senior officials in the executive branch. Steady progress has been made in recent years in rebuilding relationships between

the Defense Establishment and the academic community, and it would be tragic indeed if current controversy marked a reversal of the efforts supported by the Department of Defense in seeking a rapprochement with the academic community.

I am very pleased to state to your committee that the Department of Defense has agreed to support and cooperate in our study, as have the National Science Foundation, the AAAS, and several private foundations. The National Academy of Sciences will also contribute to the support of this study. The chairman of the panel will be Dale Corson, president emeritus of Cornell University, and a member of the National Academy of Engineering. With your permission, I would like to place in the record our announcement of this study and a list of the distinguished panelists chosen to consider this matter.

Mr. GORE. Without objection.

Dr. PRESS. The panel includes individuals fully conversant with the goals of science, the nature of universities, and issues of national security. Members have expertise in a variety of scientific and engineering disciplines, management of R. & D., trade regulation and control, and relevant legal and administrative requirements. I feel certain that the panel will provide an objective and rigorous evaluation of issues surrounding the application of controls to scientific and technological communication.

The review will consist of the following elements:

An examination of the advantages and disadvantages of free communication in two or three specific fields of science and technology, such as mathematics relating to cryptology, very high speed integrated circuits, and artificial intelligence.

A review of the policy and operational concerns of the respective government agencies, universities, scientific societies, and researchers. The goal here is to identify issues where there is common agreement, to expose those where apparent disasgreements are based on misperceptions and misunderstandings, and perhaps to narrow and sharpen the focus on issues where genuine differences exist.

The panel will conduct a rigorous evaluation of critical issues concerning the application of controls on the flow of research information, and the effects of such controls on scientific and technological progress.

Finally, the panel will develop recommendations and conclusions concerning: The intended and proper reach of controls, vis-a-vis various categories of science and technology; areas of science and technology that are or should be outside of operational controls; approaches that could provide more certainty and predictability to the regulatory system; and alternative procedures that might prove acceptable to all of the concerned sectors.

Mr. Chairman, there is one other important matter which I feel should be addressed. The Academy currently operates interacademy exchanges with the U.S.S.R. and Eastern Europe, as well as with China.

For decades, the State Department has obtained waivers to provisions of the Immigration and Naturalization Act barring U.S. entry to members of Communist parties and certain other categories of aliens, thus enabling Soviet and Eastern European participants in

the interacademy exchange program to obtain nonimmigrant visas. Prior to authorization of visas in such cases, the State Department passes judgment on the acceptability of the proposed program of the intended visitor. In years past, the clearance procedure has been relatively routine and only occasionally did significant problems for exchange administration of this program arise.

However, heightened sensitivities to technology transfer issues have led to increasing difficulties in the Soviet exchange program.

I believe that our exchange program with the Soviet Union should not provide either side with any relative advantage, that it should be balanced, with a roughly equal flow of information in both directions. I think that areas of critical technology should not be included.

That said, I think it is in our interest to cooperate with the Soviets. They are a world class scientific and technological nation. In such areas as—and I have just jotted these down—condensed matter physics, high energy physics, astrophysics, nuclear fusion for energy, MHD, earthquake prediction, electrometallurgy, certain aspects of cancer and coronary disease, and planetary exploration, the Soviets operate at our level. I believe it is in our interest to work with them in these areas where there is a mutual flow of information in both directions.

In balancing this equation, we should take into account that the social scientists that we send to the Soviet Union play an important role. There are too few Americans who speak Russian, and at the same time know the politics, the culture, the economy of Soviet institutions. I believe it is to our advantage to train such scholars by sending them to the Soviet Union, and that should be used in our equation for balancing the degree of flow of advantage in both directions.

In conclusion, I believe this study which we are undertaking in cooperation with the government provides an ample framework for an objective assessment of the relationship between national security interests and open scientific communications. I do not want to prejudge the panel's recommendations. I am sure, however, it will consider the advantages and disadvantages of exchanges with Soviet bloc countries in areas of critical technology and in basic scientific areas; review restrictions on such exchanges and whether they are justified; and evaluate the ability and willingness of universities to enforce them. It will provide an opportunity to narrow and define the issues in which genuine differences may exist in the hopes of strengthening mutual understanding and confidence.

Thank you, Mr. Chairman.

[The prepared statement and attachments of Dr. Press follows:]

STATEMENT

by

Frank Press
President
National Academy of Sciences

before the
Subcommittee on Science, Research and Technology
and
Subcommittee on Investigations and Oversight
of the
Committee on Science and Technology
U.S. House of Representatives

Hearings to ascertain the impact on science and technology of recent national security proposals

March 29, 1982
Room 2318, Rayburn House Office Building

Mr. Chairmen, thank you for the opportunity to discuss with your Subcommittees the impact on science and technology of proposed government initiatives for increasing national security restrictions over the exchange of scientific information. I am also pleased to discuss with you the cooperative role of the National Academy of Sciences in addressing these issues and in seeking an accommodation between government and the scientific research community. As your Committee has recognized, the quest for that accommodation presents difficulties in finding a balance between (a) national security and economic interests, and (b) individual rights, including those associated with open scientific communication.

The issues leading to the current controversy are not new, extending back over the past several years as public sensitivity has heightened within the United States over growing international military tensions and the increasing transfer of American technological know-how to our foreign industrial competitors. These are matters with which I have been personally concerned, not only as President of the National Academy of Sciences but also during my term as Science Advisor to the President of the United States and Director, Office of Science and Technology Policy.

Notable strides made by the Soviet Union in the military sphere have been largely responsible for increased interest in preventing the transfer of militarily sensitive products and knowledge to our nation's potential adversaries. In response to these concerns about the leakage of militarily sensitive information, various Executive Branch agencies are currently reappraising policies on the transfer of technology to foreign countries. Government officials have expressed concern in particular about foreign access to computer science and mathematics research that bears on cryptology, and to research involving magnetic-bubble memory devices, laser-optics and inertial confinement fusion, and very high speed integrated circuitry (VHSIC). Public attention also has increasingly been drawn to these matters because of the significant competitive success of major industrial countries -- success made possible in many instances by the apparent ease with which other industrial nations can draw upon the results of American research and development.

Technology transfer can take many forms that go beyond the acquisition of hardware or processes. The collection of data and information in the open literature, person-to-person scientific exchanges, attendance at conferences,

symposia, and other open forums, and participation in university research and education -- all offer the opportunity for transfer of technological data. These transfer issues pose a dilemma for the government and the university-based scientific and engineering community -- one that both parties, and the country generally, have a high stake in resolving in a mutually constructive and satisfactory manner; yet one, unhappily, in which recent developments point more toward polarization than consensus. The issue can be stated as follows.

Some government officials believe that a category of unclassified research results exists whose free and open publication or dissemination, especially to particular foreign nationals, could pose an undue threat to the national interest and, at times, to national security. Accordingly, they think it is essential to control foreign access to this information. On the other hand, most scientists and engineers in academia hold that open communication is absolutely essential for a creative research environment. In their view, restrictions on scientific communication sap the strength and vitality of the educational and research endeavors upon which the nation's present and future technology base is founded. Moreover, such restrictions

are seen as inconsistent with a free society and, in some instances, with basic constitutional rights. Neither would they like to see us forced to emulate the Soviet practice of compartmentalizing and restricting access to knowledge.

Traditional means by which the government seeks to protect and promote the nation's security and technological leadership include classification of military and diplomatic secrets; surveillance and controls of foreign visitors through visa and travel restrictions; and export control restrictions, outside the military intelligence security classification systems.

Increased controls over the transfer of sensitive technical data can be achieved either by expanding the coverage of the military and intelligence classification system, through, for example, revision of the Executive Order covering such matters, or by the more rigorous application of export controls. Expansion of the scope of classified information is highly controversial. I offer for the record a copy of a letter which I recently sent to the President's National Security Advisor on proposed changes in the Executive Order on national security information. This letter highlights the nature of these controversies from the vantage point of the scientific community.

Our major concern is that the proposed expansion of the scope of classified information into peripheral areas could force some basic scientific research indirectly relating to national security, out of most leading universities that will not do classified work, thus denying this important resource to the Defense Department. It would be unfortunate, indeed, if by these steps we discouraged major components of the scientific research community from continuing basic research in areas of potential importance to our national security. We should consider how much our security is harmed by denying government access to many of the nation's most brilliant scientists and engineers who work on university campuses.

Export controls on the transfer of technical data are equally controversial. Interpretations of export regulations are often broadly cast in ways that members of the academic community believe are unnecessarily restrictive. Technical judgments are made by persons within the government who are often perceived by scientists as lacking competence in a particular topic or discipline or who are not familiar with the nature of scientific discovery. Government officials, from their perspective, think that members of the academic community are often naive or uninformed about

Best Available Copy

the extent and consequences of technology transfer to other nations. Thus, it is important that we have a balanced and objective assessment of the views of both the government and the scientific community on these controversies.

Mr. Chairmen, the interdependence of government and the research community in advancing science, technology and the national security requires the prevention of a breakdown of mutual confidence. In February of this year, I communicated my concerns on these issues to the Under Secretary of Defense for Research and Engineering when I sought the cooperation of the Department of Defense in a study to be initiated by the National Academy on the impact upon scientific communication of government regulations concerning technology transfer. I have also discussed this matter with other senior officials in the Executive Branch. Steady progress has been made in recent years in rebuilding relationships between the defense establishment and the academic community and it would be tragic, indeed, if current controversy marked a reversal of the efforts supported by Defense in seeking a rapprochement with the academic community.

Best Available Copy

I am very pleased to state to your committee that the Department of Defense has agreed to support and cooperate in our study. The chairman of this panel will be Dale Corson, President Emeritus of Cornell University and a member of the National Academy of Engineering. With your permission, I should like to place in the record our announcement of the study and a list of the distinguished panelists chosen to consider this matter. INSERT Gor-w/o DOJ.

The panel includes individuals fully conversant with the goals of science, the nature of universities, and issues of national security. Members have expertise in a variety of scientific and engineering disciplines, management of research and development, trade regulation and control, and relevant legal and administrative requirements. I feel certain that the panel will provide an objective and rigorous evaluation of issues surrounding the application of controls to scientific and technological communication.

The review will consist of the following elements:

- An examination of the advantages and disadvantages of free communication in two or three specific fields of science and technology, such as mathematics relating to cryptology, very high speed integrated circuits, and artificial intelligence, to be selected by the study panel in consultation with the Department of Defense.

- A review of the policy and operational concerns of the respective government agencies, universities, scientific societies, and researchers. (The proprietary concerns of industry will not be considered.) The goal here is to identify issues where there is common agreement, to expose those where apparent disagreements are based on misperceptions and misunderstandings, and, perhaps, to narrow and sharpen the focus on issues where genuine differences exist.

- The panel will conduct a rigorous evaluation of critical issues concerning the application of controls on the flow of research information, and the effects of such controls on scientific and technological progress, and will

- Develop recommendations and conclusions concerning: (i) the intended and proper reach of controls vis-a-vis various categories of science and technology; (ii) areas of science and technology that are or should be outside the operation of controls; (iii) approaches that could provide more certainty and predictability to the regulatory system; and (iv) alternative procedures that might prove acceptable to all of the concerned sectors.

In this effort we will have the cooperation and support of other scientific societies and government agencies. The panel is scheduled to make a report in September and while I would not want to prejudge the results, I look for a positive outcome.

Mr. Chairmen, there is one other important matter which I feel should be addressed in my statement. The NAS currently operates interacademy exchanges with the USSR and Eastern Europe. Its Committee on Scholarly Communication with the People's Republic of China (CSCPRC) (jointly sponsored by the NAS, along with the American Council on Learned Societies and the Social Science Research Council) operates exchanges with China's Scientific and Technical Association. The USSR/Eastern Europe program consists of the exchange of visiting scholars. The program with China began with several years of exchanges of delegations, but now also involves the exchange of visiting scholars and students.

For decades, the State Department has obtained waivers to provisions of the Immigration and Naturalization Act barring U.S. entry to members of Communist parties and certain other categories of aliens, thus enabling Soviet and Eastern European participants in the interacademy exchange program to obtain nonimmigrant visas. Prior to authorization of visas in such cases, the Department of State passes judgment on the acceptability of the proposed professional program of the intended visitor. In years past, the clearance procedure has been relatively routine and only occasionally did significant problems for exchange administration arise.

However, heightened sensitivities to technology transfer issues have led to increasing difficulties in the Soviet exchange program, as illustrated by the recent case of the proposed visit of Dr. N. V. Umnov, a Soviet scientist who is one of the world's leading specialist on robotic walking machines.

In mid-December 1981, a communication went from the NAS USSR/Eastern European exchange office to laboratories at four universities (Stanford, Wisconsin, Ohio State, and Auburn) inquiring whether they had an interest in receiving an exchange visit from Dr. Umnov. The communication listed a number of restrictions that the State Department would impose on the visit, including access to certain types of university research activities and all on- or off-campus industrial facilities in his field.

Stanford replied that it would be unable to receive Dr. Umnov under those restrictions; researchers at two other universities voiced similar reservations on the grounds that the restrictions were incompatible with the openness of university life, that the restrictions were inapplicable since their universities were not involved with classified research, and that -- in any case -- a university could not be responsible for a visiting scholar's off-campus activities.

97-341 O - 82 - 6

In partial response to these questions, the Academy initiated a series of discussions with responsible officials in the State Department; the outcome was a modification of the language of the restrictions that provided a common ground apparently acceptable to both the government and the prospective host institutions. According to this restatement, Umnov would be permitted to visit any campus laboratory whose research results were intended for publication in the open literature, and the hosts would not be held responsible for controlling the off-campus activities of their visitor.

The NAS has for a number of years been routinely advising individuals at host institutions of State Department restrictions on the activities of proposed exchange visitor. But in a rapidly changing political climate, the Academy has had to deal with expanding government emphasis on security and mounting university concern about restrictions difficult or impossible to implement. Although the China exchange has not yet received the attention that has been given to the USSR/Eastern Europe program, technology transfer issues also could arise under this program. Unresolved at this point are the exact nature and extent of the liability which the State Department is seeking to impose in connection with future exchange visits.

The Academy will continue to communicate exchange visitor restrictions to potential host institutions under new internal guidelines now being developed. These guidelines will be interim in nature to be reevaluated after completion of the study which I have previously described to you.

In conclusion, I believe this study which we are undertaking in cooperation with the government provides an ample framework for an objective assessment of the relationship between national security interests and open scientific communications. I do not want to prejudge the panel's recommendations. I am sure, however, it will consider the advantages and disadvantages of exchanges with Soviet bloc countries in areas of critical technology and in other areas; review restrictions on such exchanges and whether they are justified; and evaluate the ability and willingness of universities to enforce them. It will provide an opportunity to narrow and define the issues in which genuine differences may exist and to strengthen mutual understanding and confidence.

NATIONAL ACADEMY OF SCIENCES
NATIONAL ACADEMY OF ENGINEERING INSTITUTE OF MEDICINE

COMMITTEE ON SCIENCE, ENGINEERING, AND PUBLIC POLICY

2101 CONSTITUTION AVENUE
WASHINGTON, D.C. 20418
202/334-2424

3/22/82
18 Members

PANEL ON SCIENTIFIC COMMUNICATION
AND NATIONAL SECURITY

Dr. Dale R. Corson - Chairman
President Emeritus
615 Clark Hall
Cornell University
Ithaca, NY 14853

Dr. Richard C. Atkinson, Chancellor
Q-005
University of California, San Diego
La Jolla, CA 92093

Dr. John Deutch
Dean of Science
Room 6-123
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

Dr. Robert H. Dicke
Joseph Henry Laboratories
Physics Department
Princeton University
Princeton, NJ 08544

Dr. Edward L. Ginzton
Varian Associates
611 Hansen Way
Palo Alto, CA 94303

Dr. Mary L. Good
Vice President -- Director
of Research
UOP, Inc.
Corporate Research Center
10 UOP Plaza
Algonquin & Mt. Prospect Rds.
Des Plaines, IL 60016

Dr. Norman Hackerman
President
Rice University
P. O. Box 1892
Houston, TX 77251

Dr. James R. Killian
Room 9-235
Massachusetts Inst. of Tech.
77 Massachusetts Avenue
Cambridge, MA 02139

Mr. Franklin Lindsay
Chairman, Executive Committee
ITEK Corporation
10 Maguire Road
Lexington, MA 02173

Best Available Copy

COMMITTEE MEMBERSHIP
(Cont'd.)

Richard A. Meserve, Esq.
Covington and Burling
Box 7566
1201 Pennsylvania Ave., N.W.
Washington, D.C. 20044

Dr. Wolfgang K.H. Panofsky
Director
Stanford Linear Accelerator
Center
Stanford University
P. O. Box 4349
Stanford, CA 94305

Dr. William J. Perry
Partner
Hambrecht and Quist
235 Montgomery Street
San Francisco, CA 94104

Gen. Samuel C. Phillips (ret.)
Vice President & General Manager
TRW Energy Products Group
9841 Airport Blvd., Suite 1500
Los Angeles, CA 90045

Dr. Alexander Rich
Building 16, Room 735
Massachusetts Inst. of Technology
77 Massachusetts Avenue
Cambridge, MA 02139

Dr. John D. Roberts
Gates and Crellin Laboratories
of Chemistry
California Inst. of Technology
Pasadena, CA 91125

Dr. Charles P. Slichter
Department of Physics
University of Illinois
Urbana, IL 61801

Mr. Michael I. Sovern
Office of the President
202 Low Memorial Library
Columbia University
New York, NY 10027

Dr. Elmer B. Staats
5011 Overlook Road, N.W.
Washington, D.C. 20016

Staff

Lawrence E. McCray
COSEPUP, Room NAS 286
National Academy of Sciences
2101 Constitution Avenue
Washington, D.C. 20418
(202) 334-2243

Best Available Copy

NATIONAL ACADEMY OF SCIENCES
NATIONAL ACADEMY OF ENGINEERING INSTITUTE OF MEDICINE

COMMITTEE ON SCIENCE, ENGINEERING, AND PUBLIC POLICY

2101 CONSTITUTION AVENUE
WASHINGTON, D.C. 20418
202/334-2484

STUDY BY
THE PANEL ON SCIENTIFIC
COMMUNICATION AND NATIONAL SECURITY

In recent years, the Soviet Union has made notable strides in competing with the United States in the military sphere -- strides that some fear were made possible in large measure by the harvesting of American technology. As a result, there is increased interest in preventing the transfer of militarily sensitive products and knowledge to our nation's adversaries. One aspect of this effort poses a dilemma for both the government and the research community.

On the one hand, knowledgeable government officials believe that the free availability to foreign nationals of certain unclassified research results in specific fields poses a threat to the national security. Indeed, they have evidence that the Soviet military posture has been notably strengthened by access to such information in the past. Accordingly, they believe it is essential to limit such foreign access through control of the export of scientific information.1/ Government officials have expressed concern in particular about foreign access to computer science and mathematics research that bears on cryptology, and to research involving magnetic-bubble memory devices, laser-optics and inertial-confinement fusion, and very high speed integrated circuitry (VHSIC).

1/ Such control could be achieved directly either by expanding the coverage of the military and intelligence classification system, through, for example, revision of the executive order covering such matters, or by the more rigorous application of the system of export controls, which operate independently of the classification system. The chief examples of the latter controls include the International Traffic in Arms Regulations (ITAR), administered by the Department of State, and the Export Administration Regulations (EAR), administered by the Department of Commerce. They currently encompass not only hardware, but also technical data.

Indirect control of the flow of information could be achieved by visa and travel restrictions, or by redirecting United States participation in scientific exchanges and international meetings.

On the other hand, most scientists and engineers in academia and elsewhere hold that open communication is an essential element of a creative environment. In their view, restrictions on communication would sap the strength and vitality of the educational and scientific endeavors upon which our technologies and our national defense are based. Moreover, such restrictions are seen as inconsistent with a free society.

A balanced and objective assessment of these opposing views is both necessary and timely. The interdependence of government and the research community in advancing science, technology and national security requires the prevention of a serious breakdown of mutual confidence.

The review will involve the following elements:

o An examination of the national-security interests and the interests in free communication in two or three specific fields of science and technology (e.g., cryptology, very high speed integrated circuits, artificial intelligence) to be selected by the study panel in consultation with the Department of Defense. This analysis will include an examination of the extent to which American research has been used in Soviet military programs and, if possible, a consideration of how such information was transferred. In addition, the panel will assess and compare the contribution to Soviet military strength from the transfer of research information with that arising from other means of technology transfer, such as the Soviet acquisition of American hardware.

o A review (with an emphasis on ITAR, EAR, and a proposed executive order on the classification system) of the principal policy and operational concerns of the respective government agencies, universities, scientific societies, and researchers. (The proprietary concerns of industry will not be considered.) The goal is to identify issues where common agreement exists, to expose those where apparent disagreements are based on misperceptions and misunderstandings, and, perhaps, to narrow and sharpen the issues on which genuine differences exist.

o A rigorous evaluation of critical issues concerning the application of controls on the flow of research information.2/

2/ Such issues might include:

(i) What do we know about the innovation and technology transfer process that bears on export control policies?; What is the appropriate balance between policies to stimulate and policies to protect critical technological advances?

(footnote con't)

o The development of recommendations and conclusions concerning: (i) the intended and proper reach of controls vis-a-vis various categories of science and technology; (ii) areas of science and technology that are or should be outside the operation of controls; (iii) approaches that might provide more certainty and predictability to the regulatory system; and (iv) alternative procedures that might prove acceptable to all of the concerned sectors.

The study panel for the assessment includes individuals deeply conversant with the goals of science, the nature of universities, and national security concerns. They have expertise in a variety of scientific and engineering disciplines, the management research and development, trade regulation and control, and constitutional law. Liaison members representing the respective government agencies and scientific institutions will be asked to assist the panel in its deliberations and in devising effective means for communicating its final conclusions and recommendations.

The overall effort will be 12 months in duration. The final product will be a public, unclassified report of the panel's findings and recommendations. A progress report will be prepared in September 1982.

(footnote con't)

(ii) What are the practical problems with and alternatives to requiring universities to enforce compliance by its students, faculty and visitors? Are the essential qualities of a university compromised by certain forms of regulation?

(iii) How can scientific and engineering advice contribute to the development and enforcement of more effective control regulations?

(iv) What controls on information transfer is it realistically possible to achieve in light of the number and diversity of scientists and engineers in the academe?

NATIONAL ACADEMY OF SCIENCES

OFFICE OF THE PRESIDENT
2101 CONSTITUTION AVENUE
WASHINGTON, D C 20418

February 26, 1982

The Honorable William P. Clark
Assistant to the President
for National Security Affairs
The White House
Washington, D. C. 20500

Dear Judge Clark:

I write to convey my concerns with regard to the proposed new Executive Order on national security information. We, in the Academy, have only recently been made aware of some of the specific proposals for revising present Executive Order 12065 and are concerned that some of these proposals, if adopted, could impede efforts currently under way to strengthen the relationship between the basic research community and the national defense establishment.

One of these proposals involves the deletion of the provisions now contained in Sections 1-602 through 1-604 of Executive Order 12065. Section 1-602 states that basic research information not clearly related to the national security may not be classified. Section 1-603 provides that, except with respect to the requirements of the Patent Secrecy Act of 1952, a product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under the Executive Order until and unless the government acquires a proprietary interest in the product. And Section 1-604 states that references to classified documents that do not disclose classified information may not be classified or used as a basis for classification. The stated reason for deleting all of these provisions is that "they are self-evident."

Our view is that the scientific community will take very little comfort in this rationale viewed in light of the overall tenor of the proposed Executive Order and the controversy which already exists on some leading university campuses over export control restrictions on technology transfer. Many scientists and engineers in academia hold that free and open communication is the sine qua non that promotes and perpetuates the strength and vitality of the educational and scientific endeavors upon which the nation's technological base is founded. The scientific enterprise of the Soviet Union provides a useful analogue of what can happen under a restrictive environment. It seems obvious that the compartmentalization and absence of free communication has significantly weakened Soviet scientific endeavor and the overall capacity for doing good science. Certainly we do not wish to move in that direction.

It also is our understanding that proposals have been advanced within the Administration to create a new category of classified information under the proposed Executive Order. This new category would cover information the unauthorized disclosure of which reasonably could be expected to cause loss to the United States of a technological, diplomatic, intelligence, cryptologic or military advantage. We understand that the intent in creating this new category would clearly be to extend coverage to some types of information that cannot now be classified under the present Executive Order. Moreover, the test for classification under this new category reportedly would not be potential damage to the national security but simply the amorphous concept of "protection in the interest of national security."

I assure you that from my viewpoint there is no questioning of the right of the government to protect the legitimate national security interests of our country, including important economic interests. Our major concern is that the proposed expansion of the scope of classified information into peripheral areas might force some basic scientific research indirectly relating to national security out of most leading universities that will not do classified work, and thus deny to the Defense Department

this important basic research resource. It would be unfortunate, indeed, if by these steps we discouraged major components of the scientific research community from continuing basic research in areas of potential importance to our national security.

The interdependence of government and the academic community in advancing science, technology and national security requires the prevention of a serious breakdown of mutual confidence. At this time, efforts are being made by the National Academy of Sciences and other scientific and technical organizations to establish a framework for discussion and mutual resolution of these issues. In the light of these efforts, I urge that modification of the present Executive Order in the areas described above be delayed, thus allowing time for further discussions with representatives of the scientific community.

This information is being communicated to you as a reflection of our sincere belief that the national interest necessitates that every effort should be made to clarify and resolve the concerns of both the U. S. Government and the academic community with respect to these issues.

Yours sincerely,

Frank Press

Frank Press
President

Mr. GORE. Thank you very much.

We will hold our questions until we have heard from Dr. Rosenzweig. Please proceed.

Dr. ROSENZWEIG. Thank you, Mr. Chairman.

The concern that was expressed this morning by the very interesting panel that preceded us, and that has been expressed elsewhere in the press and other places, derives in large part from the broader fact that the United States no longer enjoys the wide margin of superiority in science and technology that was ours for more than a quarter of a century following the close of World War II. It is widely believed that if we lose that advantage over our adversaries, we would face a very substantial threat to our national security.

It so happens I believe that conclusion is correct, and because it is, it is critically important that we understand the sources of our remaining advantage and that we adopt policies that will preserve it. There is some risk, I believe, that we may do just the opposite, that in our determination to maintain our edge we may choose an approach that has an attractive surface validity, but which will, in fact, have effects exactly opposite those that are intended.

The main danger, it seems to me, lies in that part of the diagnosis that ascribes the current situation to the fact that university-based science is open and its results freely available. Not the least of the consequences of that faulty diagnosis is that it could cause a bruising confrontation between the Government and universities.

Now, the specifics of that diagnosis focus first on the unbalanced nature of scientific exchanges between the United States and the Soviet Union, in which the Russians send scientists and engineers

to learn from the advanced work of American laboratories what they are apparently unable to teach themselves, and in which we send humanists and social scientists to work in those libraries and archives that the Russians are willing to hold open for us.

Second, and perhaps even more important, is the assertion that the very nature of our scientific enterprise, with its emphasis on free communication of research results, exposes our most advanced work to the eyes of anyone who is willing to pay the price of subscriptions to freely available technical journals.

I think there are probably more important explanations of the current situation and it is worth examining them briefly. It seems to me far more likely that the extraordinary dominance enjoyed by American science and technology at the close of the war was a product of the exhaustion of our enemies and our allies, and of the unparalleled flow of brilliant scientific talent fleeing from the totalitarian regimes of Europe. The recovery of the leading powers of Europe and of Japan was to be expected; the application of the talent and energy that exists in other places was bound to reduce our advantage. Moreover, those who were starting over did not have to reinvent what had already been discovered.

What is far more interesting, it seems to me, and much more relevant to current policy, is how we have managed to sustain the edge that we have over a broad range of scientific areas in spite of the energetic and determined competition by others. What, in other words, are the sources of our continuing strength? I suggest that it rests on five major elements, and I will simply list them in no particular order of importance.

First, we have an economic system that rewards and therefore encourages risk taking. Working with new technology is inherently risky. Bureaucracies, in contrast, are risk-averse. Centrally directed, and therefore highly bureaucratized, economics share that quality. On the whole, we do not, and that is a source of strength for us.

Second, we have an educational system that by and large makes it possible for talented people to go as far as their talents will take them. Thus, our pool of talent is far larger than elsewhere in the world.

Third, we have a tradition of higher education in this country that connects it with the requirements of the society it serves, while also protecting it from distortion by those same requirements. It is a tradition that is especially relevant to the health of science and technology, as shown by examples as diverse and reaching as far back in our history as the role of the land grant colleges and universities in the growth of American agriculture, the importance of the links between such universities as MIT and Stanford, and the electronics and computing industries, and the emerging set of connections between universities and industry in the field of biotechnology. There is nothing analogous to this phenomenon elsewhere.

Fourth, in this country we link fundamental research and research training. They are done in the same place, universities, and by the same people, faculty and graduate students. Indeed, the activities are simultaneous and indistinguishable. Thus, research is refreshed by the best young minds, and the best of our young are

trained by the best of our senior people. This, too, is a source of great strength.

And finally, we have a scientific structure that puts a high value on the free communication of scientific results. This has two enormously valuable sets of consequences. The first is that good people are very quickly recognized, and so are those who are less good. And second, good results can be rapidly confirmed and quickly become the platform for further work, while error can be rapidly identified and set aside. If there were no other justification for maintaining the traditional openness of our scientific work, it could be justified on the grounds of its value as an economizing device alone.

Now, any solution to the problem of technology leakage that does not take account of those elements of our strength, any solution, in short, that does damage to the sources of our strength, will produce results far worse than the problem it purports to solve. Policies aimed at protecting American security by keeping from others the fruits of our science and technology must be tested against that standard, no matter how plausible they might otherwise seem. Specifically, we should look at the two alleged causes of leakage in that light, the two that have to do with universities, I should say.

The first of those is the uneven nature of exchanges between the Soviet Union and the United States. The first thing to be said about that subject is that it is true, that we and the Russians treat these exchanges quite differently, and that they derive more tangible benefits from them than we do. That is not to say that we derive no benefits at all. As others have said, we have precious few points of access to that closed society, and while we have little to gain from their science and technology, we have much to lose from ignorance of Russian institutions, processes, motives, and purposes.

Still, there is no denying the systematic way in which the Russians plan for and profit from the opportunities afforded their people in this country. What needs to be said is the fact that its control is wholly within the powers of the U.S. Government right now. No legislation, no increase in authority is required to limit Russian access to what is deemed to be sensitive training and research. Under existing agreements, the State Department must approve the program of study of a Russian scientist before he can be assigned to an American university. If the course of study is sensitive, or is closely connected to sensitive work, the remedy is to veto the application.

Mr. GORE. Dr. Rosenzweig, if I may interrupt you there, I think there is a difference between disclosure and technology transfer. The ability of the Government to restrict entry visas for reasons of technology transfer is not as settled a question as their ability to deny a visa for someone that poses a national security risk; is that not so?

Dr. ROSENZWEIG. I believe within the context of the formal exchange agreements that have been negotiated under the Cultural Exchange Agreements, that programs of study must be approved before a visa is issued.

Mr. GORE. I'll pursue it. I shouldn't have interrupted you.

Go ahead.

Dr. ROSENZWEIG. The explanation of some recent controversies, including one in which Stanford was involved, was that the State Department proposed to admit a Russian visitor and allow him to come to Stanford, but only if we would agree to prevent him from seeing and hearing things that are perfectly open to everyone else. Moreover, we were asked to assure that he would not see any nearby businesses.

Now, in our view, that was bad policy. It was a complicated and almost certainly ineffective solution to what was really a fairly straightforward problem. If the work going on at Stanford was judged to be too sensitive to be exposed to a Russian visitor, then the solution was to keep him away from the university, not to ask the university to play policeman during his visit.

It strikes me, though, that whatever problems derive from scientific exchanges ought to be manageable. The governing principle should be that the decision about whether a particular individual proposes to pursue an inappropriate program properly belongs to the Government. Once an individual is admitted for study, however, the institution at which he is working should not be asked to become less open, more secretive.

The general problem of the ready availability of the results of American scientific research through the open literature is at once easier to comprehend and far more difficult to deal with. It is true that our scientific literature is open and freely available. It is also true that this fact enables others to profit from our work, thereby narrowing our margin of superiority. But as I have already suggested, the more important question is what accounts for our margin of superiority in the first place. If it is correct that the very openness that is to the benefit of others is also an important factor in maintaining our advantage, then we would tamper with it only at our peril.

Surprisingly, there is very substantial agreement on that point. Even those who would like to shut down the flow of certain kinds of information are usually quick to say that they do not propose programs of Government censorship or extensive new classifications of research projects. More commonly, the call is for some kind of voluntary self-regulation, a system of voluntary pre-publication screening of research results, so that findings with potential military application can be kept out of circulation.

That is a seductive notion. Indeed, in narrowly circumscribed fields of study, it might even work. Furthermore, so long as the final decision on publication remained with the scientist and not with the Government, there is no insurmountable barrier of principle. Such agreements now exist in some government and industrially sponsored research, and the field of cryptography is now engaged, as we heard, in a 2-year test of such an understanding.

Parenthetically, the question of restricting publication in order to protect patent rights is, I think, quite widely misunderstood, if I may just say a word about that here.

The purpose of the patent system, as is made abundantly clear in the Constitution, in which it's embedded, is specifically to insure the free flow of scientific and technical information. Therefore, brief delays in publication in order to allow for the filing of a patent are justified in academic terms precisely in order to make

full and free dissemination of knowledge possible; that is, to avoid the kind of secrecy that is motivated by the need to preserve a competitive advantage that can't be protected under the law.

Well, in any event, I doubt seriously that the voluntary solution has wide applicability. My sense is that the more widely agreements of that sort were to be extended, the more difficult they would be to enforce, the more frustrating the failure to abide by them would be, and the closer we would therefore be to the next steps, namely, required prescreening and Government control over the decision to publish.

I don't know anyone who now wants that result. It is important to keep in mind, however, that the impulse behind regulation of any kind, voluntary or otherwise, is a perceived threat to national security. As we heard this morning, that is a uniquely unanswerable argument. If we accept the premise that our national security is threatened by the free communication of research results, then the only policy dispute that remains is over the effectiveness of this or that means of making it less open.

I submit that the premise is wrong. We should reject it. Our security, our health, and our prosperity will be served best by adherence to the principles and practices that have been our main sources of strength.

It has always seemed risky, Mr. Chairman, to run an open society. Perhaps that is why there are so few of them. But when citizens and leaders alike have been willing to take the risk, as ours have been willing to do throughout our history, the most marvelous engine of creativity is set in motion. That, I submit, is our real advantage. Why on earth would we want to give it away?

Thank you.

[The prepared statement of Dr. Rosenzweig follows:]

TESTIMONY

of

Robert M. Rosenzweig

Vice President for Public Affairs

Stanford University

on

March 29, 1982

before the

Subcommittee on Science, Research and Technology

and the

Subcommittee on Investigations and Oversight

of the

Committee on Science and Technology

Mr. Chairman and Members of the Committee:

There is a great deal of quite understandable concern abroad these days about the fact that the United States no longer enjoys the wide margin of superiority in science and technology which was ours for more than a quarter of a century following the close of World War II.

If all that were at stake in this condition were the ability of our industry to compete with others, we would have a worrisome problem, but probably not one of such urgency as to produce the hearings of this Committee or the other evidence of acute high level attention. But more is at stake, most importantly matters of military security.

Our national history and values have always argued against maintaining large standing armed forces in peacetime. For most of our history geography compensated for that policy. It no longer does; instead its place has been taken in the front line of national defense by science and technology, and more specifically by our ability to make up for a disadvantage in numbers with the power and sophistication of the weapons in our armory. It is widely believed that, if we lose that advantage over our adversaries, we would face a very substantial threat to our national security.

I believe that conclusion is correct, and because it is, it is critically important that we understand the sources of our advantage and that we adopt policies that will preserve it. There is some risk that we may do just the opposite, that in our determination to maintain our edge we may choose an approach that has an attractive surface validity, but which will in fact have effects exactly opposite those that are intended.

97-341 O - 82 - 7

The main danger lies in that part of the diagnosis that ascribes the current situation to the fact that university-based science is open and its results freely available. Not the least of the consequences of that faulty diagnosis is that it could cause a bruising confrontation between the government and universities.

The prospect of such a confrontation should be a source of great concern. For more than thirty years the relationship between the national government and the universities of the nation has been central to the growth of our capacity to do advanced research. While there have been controversies and strains in the relationship from time to time, it would be hard to find a similarly large and complex set of governmental activities that has been conducted with such informed concern about the conditions that make the desired results possible. If important government officials act on a belief that some of those conditions, generally thought to be a scource of strength, are in fact a cause of weakness, then there is surely serious trouble ahead. The accuracy of the diagnosis is, therefore, of critical importance.

The specifics of that diagnosis focus first on the unbalanced nature of scientific exchanges between the United States and the Soviet Union in which the Russians send scientists and engineers to learn from the advanced work of American laboratories what they cannot teach themselves, and in which we send humanists and social scientists to work in the libraries and archives that the Russians are willing to hold open. Second, and perhaps even more important, is the assertion that the very nature of our scientific enterprise, with its emphasis on free communication of research results, exposes our most advanced work to the eyes of all those who are willing to pay the price of subscriptions to freely available technical journals.

Is that true? Can the development of world science and technology for the last twenty five years be explained in any significant measure by those two factors? I think that there are more important explanations, and it is worth examining them briefly.

It seems far more likely that the extraordinary dominance enjoyed by American science and technology at the close of the war was a product of the exhaustion of our enemies and our allies and of the unparalleled flow of brilliant scientific talent fleeing from the totalitarian regimes of Europe. The recovery of the leading powers of Europe and of Japan was to be expected; the application of the talent and energy that exists in other places was bound to reduce our advantage, and of course, those who were starting over did not have to reinvent what had already been discovered.

What is far more interesting, it seems to me, is how we have managed to sustain the edge over a broad range of scientific areas in spite of energetic and determined competition. What, in other words, are the sources of our continuing strength? I suggest that it rests on five major elements. I will simply list them, in no particular order of importance.

1. We have an economic system that rewards and therefore encourages risk taking. Working with new technology is inherently risky. Bureaucracies, in contrast, are risk-averse. Centrally directed, and therefore highly bureaucratized, economies share that quality. On the whole, we do not, and that is a source of strength.

2. We have an educational system that by and large makes it possible for talented people to go as far as their talents will take them. The growth of comprehensive programs of student financial aid has enabled good students and good colleges to find one another, overcoming the historic obstacle of family financial status. Thus, our pool of talent is far larger than elsewhere in the world.

3. We have a tradition of higher education in this country that connects it with the requirements of the society it serves while also protecting it from distortion by those same requirements. It is a tradition that is especially relevant to the health of science and technology, as shown by examples as diverse as the role of the Land Grant colleges and universities in the growth of American agriculture, the importance of the links between such universities as MIT and Stanford and the electronics and computing industries, and the emerging set of connections between universities and industry in the field of biotechnology. There is nothing analagous to this phenomenon elsewhere.

4. In this country we link fundamental research and research training. They are done in the same place--universities--and by the same people--faculty and graduate students. Indeed, the activities are simultaneous and indistinguishable. Thus research is refreshed by the best young minds, and the best of our young are trained by the best of our senior people. This, too, is a source of great strength.

5. Finally, we have a scientific structure that puts a high value on the free communication of scientific results. This has two enormously valuable sets of consequences. The first is that good people are very quickly recognized, and so are those who are less good. And second, good results can be rapidly confirmed and quickly become the platform for further work, while error can be rapidly identified and set aside. If there were no other justification for maintaining the traditional openness of our scientific work, it could be justified on the grounds of its value as an economizing device, alone.

Any solution to the problem of technology leakage that does not take account of those elements of our strength, any solution that does damage to the sources of our strength, will produce results far worse than the problem it purports to solve. Policies aimed at protecting American security by protecting from others the fruits of our science and technology must be tested against that standard, no matter how plausible they might otherwise seem. Specifically, we should look at the two alleged causes of leakage in that light.

The first of those is the uneven nature of exchanges between the Soviet Union and the United States. The first thing to be said about that subject is that it is true that we and the Russians treat these exchanges quite differently, and that they derive more tangible benefits from them than we do. That is not to say that we derive no benefits at all. We have precious few points of access to that closed society. While we have little to gain from their science and technology, we have much to lose from ignorance of Russian institutions, processes, motives, and purposes. It is probably true that most American specialists on the subject of Russia who are under the age of forty five, studied

and did research in the Soviet Union under the Cultural Exchange agreements. We should be wary of throwing that opportunity away.

Still, there is no denying the systematic way in which the Russians plan for and profit from the opportunities afforded their people in this country. What needs to be said about that fact is that its control is wholly within the powers of the United States government right now. No legislation, no increase in authority is required to limit Russian access to what is deemed to be sensitive training and research. All of the exchange agreements are negotiated government to government. Their terms are thus within our power to change. More to the point, under existing agreements the State Department must approve the program of study of a Russian scientist before he can be assigned to an American university. If the course of study is sensitive, or is closely connected to sensitive work, the remedy is to veto the application.

The explanation of some recent controversies, including one in which Stanford was involved, was that the State Department proposed to admit a Russian visitor and allow him to come to Stanford, but only if we would agree to prevent him from seeing and hearing things that are perfectly open to everyone else. Moreover, we were asked to assure that he would not see any nearby businesses. That was bad policy. It was a complicated and almost certainly ineffective solution to what was a fairly straightforward problem. If work going on at Stanford was judged to be too sensitive to be exposed to a Russian visitor, then the solution is to keep him away from the University, not to ask the University to play policeman.

It strikes me that whatever problems derive from scientific exchanges ought to be manageable. The governing principle should

be that the decision about whether a particular individual proposes to pursue an inappropriate program properly belongs to the government. Once an individual is admitted for study, however, the institution at which he is working should not be asked to become less open, more secretive.

The more general problem of the ready availability of the results of American scientific research through the open literature is at once easier to comprehend and far more difficult to deal with. It is true that our scientific literature is open and freely available. It is also true that this fact enables others to profit from our work, thereby narrowing our margin of superiority. But as I have already suggested, the more important question is what accounts for our margin of superiority in the first place. If it is correct that the very openness that is to the benefit of others is also an important factor in maintaining our advantage, then we would tamper with it only at our peril. The cure would surely be worse than the disease.

Surprisingly, perhaps, there is very substantial agreement on that point. Even those who would like to shut down the flow of certain kinds of information are usually quick to say that they do not propose programs of government censorship or extensive new classification of research projects. More commonly, the call is for some kind of voluntary self-regulation, a system of voluntary pre-publication screening of research results, so that findings with potential military application can be kept out of circulation.

That is a seductive notion. Indeed, in narrowly circumscribed fields of study, it might even work. Furthermore, so long as the final decision on publication remained with the scientist and not with the government, there is no insurmountable

barrier of principle. Such agreements now exist in some government and industrially-sponsored research, and the field of cryptography is now engaged in a two year test of such an understanding.

I seriously doubt, though, that it is a solution of very wide applicability. My sense is that the more widely agreements of that sort were to be extended, the more difficult they would be to enforce, the more frustrating the failure to abide by them would be, and the closer we would therefore be to the next steps, namely, required pre-screening and government control over the decision to publish. I do not know of anyone who now wants that result. It is important to keep in mind, however, that the impulse behind regulation of any kind is a perceived threat to national security. That is a uniquely unanswerable argument. If we accept the premise that our national security is threatened by the free communication that marks our system of science, then the only policy dispute is over the effectiveness of this or that means of making it less open.

I submit that the premise is wrong. We should reject it. Our security, our health, and our prosperity will be served best by adherence to the principles and practices that have been our main sources of strength. It has always seemed risky to run an open society; perhaps that is why there are so few of them. But when citizens and leaders alike have been willing to take the risk, as ours have been willing to do throughout our history, the most marvelous engine of creativity is set in motion. That is our real advantage. Why would we want to give it away?

Best Available Copy

Mr. GORE. Thank you very much.

Dr. Press, how soon can we expect the recommendations from the National Academy panel studying this matter?

Dr. PRESS. I am hopeful that most of the briefings and discussions can take place in the next month or two, so that by September we could have a presentation to the Government about what we found out and what our views are, in an interim fashion may be very close to our final report as well.

Mr. GORE. I wonder if you could come back to another joint hearing of these two subcommittees when that report is complete?

Dr. PRESS. I would be happy to.

Mr. GORE. Dr. Rosenzweig, among the many questions I want to address to you and to Dr. Press, let me go first to the one that you alluded to just briefly with your statement on patents assuring the free flow of information.

Of course, while that's true, that is far from the extent of the threat posed to academic freedom by the contractual arrangements that you and I have discussed on several occasions; you would agree with that, wouldn't you?

Dr. ROSENZWEIG. Yes, I would.

Mr. GORE. Were you surprised to hear Admiral Inman and Secretary Brady say that the willingness of the academic community to accept restraints on the traditional view of academic freedom in the name of preserving contractual arrangements with businesses in part led them to see the need, perhaps the viability, of similar restraints, where the Government's national security interests were involved? Were you surprised to hear them say that?

Dr. ROSENZWEIG. No, I was not. There is an apparent kind of symmetry there. Admiral Inman at several points took pains to make clear what he actually said as opposed to what he was reported as saying. I think I can help him on this point.

What he actually said in that talk, primarily at least, had to do with the consulting arrangements of faculty, rather than the contracts for research between universities and industry. It is true, that in their individual consulting arrangements faculty frequently undertake to maintain a confidentiality or a secrecy in ways that are quite inappropriate in the context of an agreement between a university and a business enterprise, in which graduate students are involved, in which publications are expected to emerge.

Even in that latter point—as you may know, I was involved over the weekend in a meeting at Paharo Dunes, which produced a set of statements which were reported in the press yesterday and this morning, on the subject of biotechnology. The subject of secrecy was discussed, I would say, in quantitative terms, as much as or more than any other single subject that was addressed. There was widespread agreement among the university presidents and other university administrators, among the faculty who were present, and among the businessmen who were present, that there is no significant advantage to business in the kind of secrecy that most people are concerned about. They do want enough time for protection of their patent interests. They don't have any significant interest in having universities protect trade secrets and other unprotectable kinds of infrmation and, in fact, would typically be rather re-

luctant to make that information available to universities in the context of these agreements.

Indeed, the agreement on the necessity to avoid secrecy was not only the first in order or presentation in the document, but I think was central to everything else that followed from it.

Mr. GORE. I want to commend you and Dr. Kennedy at Stanford for hosting that meeting. Of course, you and I have had a number of private meetings about how the university community might go forward in this area. But I am concerned that when you have scientific conferences and corporate lawyers review the presentations made at academic conferences for disclosure of trade secrets, that the cross-fertilization that my colleague from Ohio mentioned earlier just doesn't take place in the same way that it might otherwise.

Dr. ROSENZWEIG. I don't mean to say there are no problems, and I think it may help to be a little more precise about what they are.

Specifically with respect to publication, I think it is generally agreed there is little, if any, problem. That is to say, our licensing people at Stanford assert categorically that they can move to protect the patent on an invention faster than any scientific journal can publish, so there is no conflict between publication and protection of patentable information.

There is a special problem that has to do with the presentation of research results in non-publishable form, either in seminars that are open to the public, or in scientific conferences. It is not clear that there is a useful university policy that governs that. The universities that were present at that meeting certainly all would articulate as a matter of policy that it is not desirable to encourage delays for that purpose. They all recognize, though, that they're dealing with individual faculty members, some of whom would be secretive if there were no commercial motive at all. I mean, it's just in the nature of their personality structure as scientists to with-hold more than others do.

It is hardly conceivable that President Kennedy or Derek Bok or the other presidents who were there would instruct their administrators to go to their faculty and say "please don't give that paper" in order to protect some commercial interest. I mean, that just doesn't happen in a respectable university—and most universities are respectable, most of the time.

So there are some special problems involved, but I think it is not as broad and general a problem as it may have been thought to be.

Mr. GORE. It seems to me that universities charged with safeguarding the great heritage they have are rightly concerned about a threat to academic freedom which may come from statements by the national security apparatus, also ought to be concerned about the threats to academic freedom resulting from a trend of much closer relationships between universities and corporations.

Dr. ROSENZWEIG. Yes.

Mr. GORE. You're from a university that has recognized that concern. Many others have not. I wish that more would. We are going to pursue that issue as well.

I wanted to briefly follow up on the ability of the Government to deny visas to scientists in exchange arrangements when a technology transfer threat is imposed.

I agree with your interpretation of the law, that they can do so. When I interrupted your prepared remarks, the point I was trying to make is that there is disagreement in the executive branch about what is required to deny a visa to a visiting scientist from a foreign country if there is a specific technology transfer threat associated with that visit.

I agree with you, that if the Government has that concern, it should not shift the burden of policing that individual's activities to universities that are not used to playing such a role, but rather should do a better job of controlling access to the country of people who may be coming here for that specific purpose, if, in fact the Government decides that it's a problem in a particular situation.

I take it that both of you would agree that the university community could be more sensitive than it is to the problem that Admiral Inman was describing. Is that an awkward way to put it, or—Yes, Dr. Press.

Dr. PRESS. Well, I think it is important for us to receive the kind of briefing that he referred to. I haven't seen the classified information that you have seen. I would like to hear him make his case about the degree of damage, even though he said it was a very small percentage. I am sure the panel we are establishing will have access to that information and will receive a briefing.

Absent that information, it is hard to take a position on what is the relative damage to our security as compared to the damage to our own institutions by proposed restriction, voluntary or otherwise.

Mr. GORE. Dr. Rosenzweig?

Dr. ROSENZWEIG. I agree with that.

Mr. GORE. OK. Mr. Brown?

Mr. BROWN. Gentlemen, I raised the point with Admiral Inman with regard to his statement on the current outflow of technological and scientific information, in which he said that this was damaging to the national interest and to the national security. I want to raise with you the question of how you distinguish between national interest and national security.

Is there a clearly defined, straightforward concept of the national interest that you gentlemen are aware of and are prepared to explain to me?

Dr. ROSENZWEIG. I would answer that "No." I think it is easier to talk about the national security than it is to talk about the national interest. National interest, like public interest, like a lot of other terms that are used frequently, tends to be used to describe the position of the speaker rather than some external reality that we can find out there. It's a difficult area.

I have not, by the way, once—and I hope it has been noticed—used the term "academic freedom" in my remarks. My position is that a genuine concern for national security leads one to the conclusion that the way we do business in this country is the best protection for our continued national security that we can find, and that departures from that way are shortsighted and liable to do more damage than good.

Dr. PRESS. If I may respond in another way, there is a narrow approach for describing national security stated in terms of specific Soviet military systems that have integrated circuits, that were de-

signed primarily by us, and that were obtained by them in some clandestine way or another. On the other hand, I believe we should take a broader view of our national security, which recognizes, for example, the role that university research plays and the contributions that university research plays and the contribution that university research make to our national security. The basic concept of the computer and the stored program computer, communications theory, new kinds of materials, represents fields of research being developed on university campuses. The semiconductor industry itself recognizes that it is underinvested in basic research and it is now turning to universities to undertake that research with industry support. So these universities are a valuable national resource and here again we should balance the equation of informational leakage on one side against the enormous contribution the universities make in their open and unrestricted research to support our national security.

Mr. BROWN. As long as we're speaking about that, Admiral Inman is going to provide us with more detailed information about the losses that are potential with regard to certain militarily sensitive technologies, or is going to try to list those for some of us.

I have not seen well quantified the advantages from maintaining a balance, let's say, more in the line of open communication. Both of you have made very effective statements on that.

Dr. Rosenzweig, you made what I thought was an excellent statement in an article that you wrote for the Mercury News, in which you quoted one of our eminent science writers along the following lines: "The reason we are ahead of the Soviets in science and technology has nothing to do with expenditures, talent or ambition, and all three departments of the United States and the Soviet Union are lookalikes. What sets the two countries apart and makes the U.S. dynamic and creative and the Soviet Union clumsy and needful of scientific larceny is that our research is mostly open and theirs is mostly secret. That is the unanimous report from emigres, defectors and foreigners who have visited Soviet research centers." Those weren't your words, of course, but you quoted them with presumed approval.

Does that still represent your views?

Dr. ROSENZWEIG. Yes, it certainly does. I don't ordinarily—I am happy to quote Dan Greenberg—but I don't ordinarily quote Edward Teller. But, as you know, he has been eloquent in his comments on this issue, specifically in his observation that the area in which we have the least lead, and which we may even be behind the Soviet Union, namely, nuclear technology, weapons technology, is the area that is hedged most around with secrecy.

People say there is some connection between those two. I don't know that they are connected. It's an interesting observation.

Mr. BROWN. Well, as you point out, it is true that the original legislation with regard to atomic energy prescribes some of the most rigorous standards for secrecy that are available to any sector of technology in this country. It is hard for me to understand your statement, therefore, that the Russians are ahead of us in this area.

Are you prepared to validate that?

Dr. ROSENZWEIG. I only know what I read in the newspapers on that subject, Mr. Brown.

Mr. BROWN. Are you hinting or, by parallelism, implying that if we rigorously enforce additional secrecy in other areas that we may similarly fall behind the Russians?

Dr. ROSENZWEIG. Yes.

Mr. BROWN. You're speaking as a political scientist, of course.

Dr. ROSENZWEIG. That's correct, which is to say a nonscientist. [Laughter.]

Mr. BROWN. That's the view of this administration, of course.

I want to go back to the statement about the national interest. It seems to me that some of our concerns about restriction on the flow of scientific information and technology stems from a concept of national interest rather than national security—and I am not implying that this is bad. But I would like to refresh your memory and ask for you to comment on the fact that President Carter felt that our national interest required us to cutoff shipments of grain to the U.S.S.R.; President Reagan felt our national interest required us to resume shipment. Likewise, President Carter felt that it was in our national interest to provide technology for, say, natural gas pipeline laying equipment, and President Reagan feels that it is in our national interest to cut off that kind of technology.

The point of this is, obviously, that when you start talking in terms of national interest, you have a much wider range of disagreement as to what the national interest is, and a much greater need for the involvement of a knowledgeable policymaking body of some sort in reaching a consensus on this.

Would you agree or disagree with that statement?

Dr. ROSENZWEIG. I would like to distinguish, in response to that, quite sharply between the situation with respect to scientific and academic exchanges and a situation with respect to the way in which we conduct our own scientific apparatus establishment in this country.

The exchange agreements, it seems to me, have always been, were in their initial impulse, and have been in their operations over the years, to a large degree, political, that is to say, an instrument of diplomatic relations between the United States and the Soviet Union. Now, they have had important academic values and other things associated with them, but they have been turned on when things have been going well, and shut down when things are going badly. Kinds of restrictions of the pettiest nature have been imposed on our people by the Soviet Union and on their people by us in return.

I just don't see those as fundamental to the American academic enterprise, although I strongly believe in the intrinsic value of a free exchange of science, since I don't think that science is a national enterprise particularly; it is, more than almost anything else, properly conceived an international enterprise. But realism dictates that we just have to look at this subset of that in more political terms than we do others, and therefore I am less troubled by hedges on those programs than I am about efforts to change in very important ways, indeed, in fundamental ways, the way in which knowledge advances best.

It strikes me that the evidence is overwhelming that knowledge advances best when the communication of knowledge is freest and most open. I can't give you numbers to prove that, but I can ask you to view evidence of our senses.

Mr. BROWN. I am sorry that you can't give us numbers because I am hoping that you or other witnesses can help us to at least define these advantages as fully as possible, because obviously, they are an essential ingredient in the balancing process that has to take place here.

Dr. ROSENZWEIG. It's possible that others can. I am simply saying I am not able to do it.

Dr. PRESS. There is no question, Mr. Brown, about the political nature of some of our cooperative agreements with other countries. I am told of one former Secretary of State who signed a science cooperation agreement every time he landed for a refueling stop.

But by and large, the scientific community itself supports these agreements for the simple reason that communication, the sharing of results, makes their own work more effective. That has been so, and it can be documented, case history after case history.

Consider the area that you're familiar with, nuclear fusion. Tocomac is a Russian word. Some of the original theoretical concepts were brought here by Soviet scientists. At one time in our exchange program the Soviets were telling us things about nuclear fusion that we had classified. That's an example of where two advanced nations working together can push more rapidly a technology that may be extremely important to the future of our world; namely, an alternate source of energy when our fossil fuels are gone.

So it is true that we have these political motivations and it is true that the budget to a certain extent goes up and down with the atmospherics, but I think one shouldn't underestimate the value that scientists recognize in this; namely, working together does make the global productivity in science more effective.

Mr. BROWN. Well, I am just trying to elaborate on the distinction, if there is one, between the concept of national interest, which does allow for some of this tit-for-tat kind of thing, and national security, which presumably is a standard which doesn't allow for that.

Of course, I think the IIASA case at present is one of those which, as Admiral Inman pointed out, is not strictly a security matter. It is slightly involved, perhaps. But the concept is being advanced here that the national interest dictates or at least leads us to sever this particular relation.

I would suggest that that's a perfectly legitimate position to take, if you agree with the particular political philosophy behind it. Even the Academy has not been above doing a little tit for tat in connection with cutting off or reducing scientific exchanges in an effort to get the attention of the Soviet Government. Am I correct?

Dr. PRESS. Are you referring to the human rights question?

Mr. BROWN. Correct.

Dr. PRESS. Yes; that's correct.

Mr. BROWN. So we're not talking about absolute principle. We're talking about a matter again of balance within the confines of a particular political philosophy.

Dr. PRESS. Human rights is an issue that is a matter of principle.

Mr. BROWN. Well, let's say a conflict of two principles.

Dr. PRESS. That's right.

Mr. BROWN. Thank you, Mr. Chairman.

Mr. GORE. Mr. Shamansky.

Mr. SHAMANSKY. Thank you, Mr. Chairman.

Dr. Rosenzweig, I found your testimony both eloquent and, of course, excellent. I am glad to have heard it.

Dr. ROSENZWEIG. Thank you.

Mr. SHAMANSKY. Having previously described my home as the location of Ohio State and Battelle and Chemical Abstracts, we also have other information industry units like Compu-Serve which serves the insurance business, and Bank One which does the computer work for Merrill Lynch, and a number of others—Wonderamics Cube started the two-way, interactive TV.

What I am getting at is that it is my understanding that in the area of cryptology, it is going to become important in the future for methods to be devised to protect legitimately the information of these various clients of these organizations that I'm referring to here.

Do either you or Dr. Press have any information or an opinion as to how well this cryptology thing working? Admiral Inman cited it as being a glowing example of what he had in mind. I accepted that initially. Is it so good, in your opinion?

Dr. ROSENZWEIG. I think Admiral Inman's conclusions may be premature on that. He may well be right, but it's early to say.

I had occasion over the weekend to talk quite a bit with Chancellor Heyman from the University of California, Berkeley, who was the chairman of the committee that put this together, and it is quite clear that the members of the committee—at least the academic members of the committee who were involved in making this arrangement—were not unanimously persuaded that it was necessary or desirable. What they said essentially was that "we are told that there is a problem here. We are not in a position to validate the existence of that problem ourselves, because the evidence for it can't be given to us, but we are willing to assume that the people who tell us there is a problem are right; therefore, what can we do to find out experimentally whether the problem exists, and if so, how great it is, and if so, whether trying to solve that problem will do more harm than good."

So they set up a system in which this very narrowly circumscribed field of people—I mean, everybody in that field knows everybody else; it's not a very large field of science—agreed voluntarily to submit their papers for review to NSA, I guess it is, or whoever their contract monitor was. If they were asked to withhold that paper, or change it, in part, they had the right to appeal that decision to an impartial board, which consisted of a group of scientists and a group of Government people, who evaluated the claims of the Government and the claims of the scientists, and reached a conclusion, which the scientist was able to accept or reject, and in the end publish if he or she chose to.

There are several things to be said about that. It's a very cumbersome arrangement, obviously. If you extend that over many

areas of science and much larger numbers of scientists, you have an administrative problem of very substantial dimensions.

The second thing is that it was established for either a 2- or 3-year experimental period. They just finished the first year, and the evidence is quite ambiguous, I think, about the extent to which there is a problem, as evidenced by the number of papers that have been challenged, and the extent to which the members of the community have been willing to agree to it and the way the apparatus is working. So it's an interesting experiment but I don't think it ought to be used for anything more than that at this point. I think it's a mistake to overlearn from that experience and to extend it prematurely to much broader areas of science and technology.

That's my own sense of that situation.

Mr. SHAMANSKY. Dr. Press, you have a more scientific, as distinguished from the unscientific, political science field, and I am concerned, as I mentioned a moment ago, about being able to improve the cryptological science. I think it is an important science and would have important applicability to the flow of information, the successful flow of information by those companies and entities that work in that area. That's very important in my home community.

Do you share the feeling that I'm getting here, that these restrictions may end up hurting us more than it hurts those we're trying to deny the information to?

Dr. PRESS. I think that the point you make, that cryptological research has a private sector, nongovernmental sector of interest, of large commercial value, is a good one. That is the case for the reasons you cited.

Also, that kind of research is a legitimate branch of pure mathematics. Factoring large prime numbers is something that mathematicians have worked on for a long time. So you're entering now the area of pure mathematics, and because there's a possible connection, there are possible restrictions on it.

I am told that in the first 30 papers submitted for clearance, all 30 were cleared within 30 days, 30-30. So, far it seems, there has been hardly any effect on research in that area.

I should point out there are a number of universities who refused to subscribe to this experiment as a matter of principle and because of concern over proposals to extend it into other areas. I would like to suspend judgment and see what happens in the next year. If it extends into other areas, I would then begin to worry.

I don't think one should, as a matter of principle, rule out possible restrictions in extremely rare cases, very rare cases, where the national security can demonstrably be shown to be at risk. One should hear the case on both sides. But if this were a way of life, extended to more than extremely rare examples, then there would be some cause for concern.

I believe the Government witnesses had in mind only a few technologies and they would claim that their application of possible restrictions would be rarely invoked. But to what extent that will occur, what they mean by that, I think those are the issues that we will be exploring in our study in the months ahead.

Mr. SHAMANSKY. Are you familiar with any explicit cases in which there has been a gross disclosure of something on which

there would have been unanimous agreement that it should not have been disclosed in the first place?

Dr. PRESS. From universities?

Mr. SHAMANSKY. Yes, or even anyplace.

Dr. PRESS. In terms of industrial concerns, the clandestine transfer of hardware, of microprocessors and that sort of thing, I believe that has occurred. In terms of the kind of research that goes on in universities, where you are not dealing with state-of-the-art manufacturing know-how in critical technologies, which was Mr. Brady's concern, I would be surprised if serious damage has been done to our country.

But again, I would like to have the briefing that we've heard about, that claims a small amount of damage has occurred.

Mr. SHAMANSKY. The matter of espionage, whether it be industrial or military, it seems to me that is a problem at all times anyway. Do you think the kind of procedures hinted at by the admiral would in any way lessen the——

Dr. PRESS. There is one way to be sure to minimize the damage from such espionage, and that is to stay ahead, by making the proper investments in R. & D. and education, capital investments in productivity, and so forth. That is how we have successfully stayed ahead in the past. If we can get our institutions in order and maintain our scientific and technological leadership, I would personally have a greater sense of security concerning our efforts in these areas.

However, as I said before, I would want to hear the Government's claims concerning the damage that has been done.

Mr. SHAMANSKY. Thank you very much, gentlemen.

Thank you very much, Mr. Chairman.

Mr. GORE. Thank you.

Dr. Rosenzweig, I would like to ask you to express for me what you believe the reaction of the university community was to Admiral Inman's initial statement and the way it was perceived.

You said in your testimony that the last 30 years of Government-university relationships have been assisted by a rare degree of understanding and sensitivity on the part of the Government. I take it that you felt the recent events eroded that relationship.

What was your reaction to the statement, at least as it was reported?

Dr. ROSENZWEIG. I missed the disclaimer that Admiral Inman said he started his speech with; namely, that he was speaking as a private citizen.

Mr. GORE. Were you at the meeting?

Dr. ROSENZWEIG. I was not at the meeting, but I read the full text of the speech afterward.

I must say that I wouldn't have been, I don't think, terribly impressed by that disclaimer, since I don't think it is possible for the Deputy Director of the CIA to speak on an issue of substantial interest to his public responsibilities as a private citizen, any more than a university president can speak on an issue of educational policy as a private citizen. You are your role, to some extent, and that's just a fact of life.

I was very much concerned about some of the things that Admiral Inman said, in the surrounding context in which Under Secre-

97-341 0 - 82 - 8

tary Carlucci had been saying similar things, and in which Secretary Weinberger had been saying things that sounded similar. My concern was that people in high positions in Government were responding to a problem by reaching for what was superficially the simplest solution to it—"if somebody is getting what we have, then keep it away from them." That struck me as a wrong and dangerous solution to the real problem, which is, properly stated, I believe, how is it that we have what we have and they don't have it, and what can we do to maintain that advantage. Looked at that way, I think you come up with a different set of solutions.

Mr. GORE. What was your reaction to his statement here this morning?

Dr. ROSENZWEIG. Well, I guess I'm not enormously reassured. I don't think—I have no reason to believe that Admiral Inman has any less concern for the values that I believe in than I do. I think he has another set of concerns that compete with those values and may override them. I worried about his expressed concern about what may happen 6 months or 12 months or 18 months from now if this hemorrhage is not staunched.

I would put it at this point at the level of concern rather than alarm. I also find a good deal of very helpful response from the community at large and from the political community. These hearings are an evidence of that response. So I don't see us barreling down a one-track railroad with nothing in sight except disaster at the other end of the line. I think we're engaging in a process here that has some controls in it, and if we're alert and vigorous to our own interests, we can probably help to shape that.

Mr. GORE. Well, it is the hope of these two subcommittees that a dialog like this one can lead to a better result than might otherwise be the case.

One final question, Dr. Press. What do you view as the appropriate role of the National Academy of Sciences in mediating or refereeing disputes of this kind? Have you been put in the middle when you don't want to?

Dr. PRESS. I don't think we want to mediate or referee at all. I believe we want to understand these issues, the constitutional questions, the questions of the nature of science and how science is impeded by certain kinds of restrictions, national interest in the broadest views that Mr. Brown has defined, and then provide suggestions and recommendations to both universities and the Government on reaching a degree of accommodation, if that's necessary.

But we are a private organization, not a governmental agency, even though Congress did give us a charter back in 1863, and I am even worried about playing the role of an honest broker, because honest brokers usually get squeezed by both sides.

However, I think the nature of our panel, the wisdom represented by the membership on that panel, is such that both sides will seriously consider their recommendations. That, is the essence of what our contribution will represent.

Mr. GORE. Well, we will look forward to hearing back from you when your panel has completed its work.

I would like to thank both of you for a very eloquent and effective statement. Thank you very much.

Dr. ROSENZWEIG. Thank you, Mr. Chairman.

Mr. GORE. Before calling our final panel, I would like to have about a 5-minute recess, no longer than that, and if our next panel could work their way to the witness table in the intervening recess, we will come back in 5 minutes.

[Recess.]

Mr. GORE. The subcommittee will come back to order.

We would like to call our third panel, Dr. Robert Corell, director of the sea grant and marine programs at the University of New Hampshire, and also representing the National Association of State Universities and Land-Grant Colleges, and the Sea Grant Association; Dr. Edward Gerjuoy, professor of physics at the University of Pittsburgh, who is also representing the American Physical Society; and Dr. John McLucas, president of the World Systems Division at Comsat.

Gentlemen, we would like to welcome all three of you. Without objection, the entire text of your prepared remarks will be included in the record in full at this point. We invite you to summarize or to present your statements in such a fashion as you see fit, beginning with you, Dr. Corell.

STATEMENTS OF DR. ROBERT CORELL, DIRECTOR, SEA GRANT AND MARINE PROGRAMS, UNIVERSITY OF NEW HAMPSHIRE; DR. EDWARD GERJUOY, PROFESSOR OF PHYSICS, UNIVERSITY OF PITTSBURGH; AND DR. JOHN McLUCAS, PRESIDENT, WORLD SYSTEMS DIVISION, COMSAT

Dr. CORELL. Thank you very much, Chairman Gore, and committee members. I do appreciate the opportunity to appear before you today to discuss a number of these vital questions that have already been addressed with such care and eloquence.

While from my perspective the impetus for these discussions emanates from the drafting of a new Executive Order with regard to national security information, it is clear that the issues being addressed have much broader origins.

As you indicated, I am here in behalf of the National Association of State Universities and Land-Grant Colleges, as well as the Sea Grant Association, the tradition of which is well known to this committee. The sea-grant colleges, on the other hand, are somewhat younger in their origin, as they are dedicated to research, education, and public service with respect to our ocean resources.

Further, to provide another context, I am a professor of mechanical engineering at the University of New Hampshire, as well as directing its marine and sea-grant college programs and, maybe more importantly to this discussion, conduct a major research laboratory that is dedicated to high technology with particular focus on underwater robotics for ocean science, military applications, and industrial utilization. It is from these vantage points that I wish to address you today.

Executive Order 12065 and its related laws and regulations provide a broad spectrum of authority for Federal agencies to control national security information, both generated within and outside the Government. The balancing test inherent in Executive Order 12065 in my opinion provides the essential context for determining access to vital information. I strongly feel that the test is crucial, a

crucial mechanism for maintaining our national security, while at the same time providing for an informed and knowledgeable citizenry.

The negative impact American universities and colleges would feel as a result of the trends in information control suggested by the draft Executive Order, and by related controls being implemented by the executive branch of Government, in my opinion, will be profound. Our Nation has grown and prospered because of its science and technology, the preeminence of which has depended historically upon the free flow and open exchange which has been well documented by other testimony, in my opinion, this morning. Without this free flow of information, the development of new knowledge and competitive technology I believe will be extraordinarily difficult. Extensive testimony to this Congress and many documents attest to that assertion.

Recent trends in reducing access to vital information related to our national security has certainly given rise to a substantial national concern. The Congress, as evidenced by this and other hearings, the National Academy, the AAAS, the Defense Science Board, the professional societies, the press, to only mention a few, each are addressing these issues with serious concern.

At the base of all this, in my mind, is a very crucial idea. It is that information is itself knowledge. Even more importantly, the very power that enables institutions to function is based upon that knowledge. Governments function because of knowledge derived from vital information. Industries grow and expand because of the information-knowledge connection. We, as private citizens, live our lives more creatively, effectively, and productively if we have open access to information and the knowledge generated therefrom. In my opinion, the genesis of the national concern over the draft order and reduced access to information is this information-knowledge-power triad.

Several weeks ago I became aware of a revised Executive Order. After reviewing a draft, I became acutely aware of a dramatic change in the tone of that order and of its fundamental hypothesis. The draft reverses trends well established by the three previous Executive Orders.

The record in the Congress concerning these vital matters has been well established and documented. For example, the Committee on Governmental Operations held a hearing on March 10 that provide substantial and well-articulated testimony about the crucial issues relating to the draft order. I would like to note particularly the testimony of Prof. Mary M. Cheh. She spoke insightfully about the problems that grow out of this new draft. She discussed effectively the dangers of erring in the direction of secrecy. The Congressional Record, containing testimony of individuals on this committee and others, is filled with many excellent examples of the problems that access to national security information is posing for our Nation.

If one could be assured that national security information were to be classified in only those cases which clearly and unquestionably threaten our national security, and further, if there was a clear and common understanding of what we mean by national security,

I don't think we would be here today. It is the human interpretation of that matter that complicates this whole issue.

There are some sectors of our society that feel that new and substantial restrictions are required to protect the security of our Nation. Others feel that openness is the central ingredient to national growth, development, and even survival. These are tough questions, I believe, and maybe even unanswerable ones. Therefore, Mr. Chairman, and committee members, I would like to propose a relatively simple but, I hope, constructive suggestion.

We engaged in a life-threatening war about 40 years ago. During that time, the role and importance of national security information became crystal clear. In the world of nations, we were young, and in many ways extraordinarily naive, concerning the relationship between information and national security. As a consequence, laws were passed and a first Executive Order on National Security was written. In the ensuing time, other pieces of legislation were enacted, well known to this committee, from the Invention Secrecy Act of 1951 through the Export Administration Act and many others. These have been Government's response to a need to effectively control information and, I believe, therefore, knowledge, to our best national interest. I suggest that each of these acts, regulations and Executive Orders were often prepared in direct response to some specific problem deemed vital to our national security.

Since World War II those items of information vital to our national security, and those items of information vital to the growth and vitality of our Nation, have become so intertwined that it is almost impossible to separate them. The distinction is almost imperceptible. The simplicity inherent in a World War II intelligence problem is no longer present in a world filled with high technology, computer systems, complex manufacturing systems, sophisticated communication capabilities, microelectronics, and the like. In short, that information which is vital to our national security is also vital throughout the industries and institutions of our country.

It is out of these perspectives that I believe it is time to pause, not to pass or issue new Executive orders, or suggest new pieces of legislation to control information, but to place the highest priority on a far-reaching national assessment of the role that information has in our national security and will have in the future vitality of this democracy. I suggest the Congress, in concert with the President of the United States, establish a national commission to address the problems we are discussing today. Such would provide structure and form to the issues that we are addressing on a nationwide basis.

The commission might examine the various laws, orders, and acts which bear upon these issues and draw out those essential ingredients that truly affect our national security. Only after a careful analysis will we be able to insure that regulations protect that which needs protection, leaving the greatest possible latitude for intellectual, economic, and social development. A thoughtful and comprehensive assessment will provide the foundations that will determine the health and strength of our country for generations to come, I believe.

Such a commission would necessarily be composed of the Congress, the judiciary, the military planners, members of the national

security community, leaders of industry and government, representatives of the academic world, the free press, and other equally important sectors of this Nation.

I wish to support strongly the study of the National Academy of Sciences and do not wish that this suggestion detract from the importance of that. In fact, it could build upon and benefit substantially by the work of the National Academy.

The timing is right, and the needs are clear. Many sectors of our society are vitally concerned that these issues be fully addressed and resolved. The concern which has been so strongly expressed during the past weeks suggest we cease an opportunity to bring a sense of wholeness to our national security information problems, instead of the piecemeal approach that I perceive to have taken place in the past four decades. The work of such a commission could lead to regulations that could effectively address our national security needs while neither undermining the fundamental precepts of our democracy nor inhibiting the growth of science and technology. In my opinion, this should be given the highest priority of Government and should be addressed immediately.

I am very grateful for the opportunity to meet and talk with you today. As I have prepared for this session, I have been increasingly overwhelmed by the fundamental nature of the discussions in which we are engaged. It is my sincere hope that the collective wisdom of Congress can be brought to bear in such a way that we address these issues directly and comprehensively, and that out of these hearings and the actions that I hope you and your colleagues will take, our Nation will bring unity and a national understanding to the control of national security information and its subsequent impact on the knowledge base of our country.

Thank you.

[The prepared statement of Dr. Corell follows:]

TESTIMONY

SUBMITTED TO THE

JOINT HEARINGS

OF THE

INVESTIGATIONS AND OVERSIGHT SUBCOMMITTEE

AND THE

SCIENCE, RESEARCH AND TECHNOLOGY SUBCOMMITTEE

OF THE

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

March 29, 1982

By

Robert W. Corell
Professor of Mechanical Engineering
and
Director of Sea Grant and Marine Programs
University of New Hampshire

On Behalf of

The National Association of State Universities and
Land-Grant Colleges
and
The Sea Grant Association

Washington, DC

I. Introductory Remarks

Chairman Walgren, Chairman Gore, and Committee Members. Thank you for the opportunity to address several vital questions concerning the impact of national secruity information policy on science and technology in our country. While the impetus for these discussions is the drafting of a new executive order to replace E.O.12065, the issues have many other origins.

I am here in behalf of the interests and concerns of the National Association of State Universities and Land Grant Colleges and of the Sea Grant Asssociation. As many of you know, the Land Grant Association is the oldest higher education association and is composed of the major public universities and colleges in every state of our nation -- 140 of them dedicated to research, education, and public service programs. The tradition of the land grant university is well known to this committee. The Sea Grant Association, somewhat younger in its origins, is composed of about 40 colleges, universities, and several industries dedicated to research, education, and public service, focused on the wise development and management of our nation's ocean resources.

Personally, I am a Professor of Mechanical Engineering at the University of New Hampshire where I also direct the Marine and Sea Grant Programs, and a major research laboratory of my own that is dedicated to the development of high technology associated with underwater robotics for ocean science, military applications, and industrial utilization. Finally, I hold, and use in my work with the U.S. Navy, a Secret Clearance. It is from these several vantage points that I appear before you to discuss these vital questions concerning national security information.

II. Crucial Issues

Executive order 12065 and several related laws and regulations provide a broad spectrum of authority to federal agencies to control national security information generated both within and outside the government . The "balancing test," outlined in the preamble to E.O.12065, provides the essential context for determining the access to vital information. I strongly feel that that test is the crucial mechanism for maintaining an informed and knowledgeable citizenry: the hallmark of our nation's heritage and of our society today.

The negative impact American universities and colleges would feel as a result of trends in information control suggested by the draft Executive Order and by related controls being implemented by the Executive Branch would be profound. Our nation has grown and prospered because of its science and technology, the preeminence of which has depended, in my opinion, upon the free flow and open exchange of information within our society and with allies and friends around the world. Without

this free flow of information, development of new knowledge and competitive technology is extraordinarily difficult. Extensive testimony and many documents attest to these assertions (Ref. 1-7). In a broader context, James Madison said it well, "Knowledge will forever govern ignorance, and a people who mean to be their own governors, must arm themselves with the power knowledge gives. A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both."

Recent trends in reducing access to vital information related to our national security has given rise to substantial national concern (Ref. 8-18). The Congress, the National Academy of Sciences (Ref. 19), the AAAS, the Defense Science Board (Ref. 20), professional societies, and the press, to mention only a few, are each addressing these issues with serious concern. The crucial issue is this: in reality information is knowledge itself. Even more importantly the very power that enables institutions to function is based on that knowledge. Governments function because of knowledge derived from vital information. Industries grow and expand because of the information-knowledge connection, and we, as private citizens, live our lives more creatively, effectively, and productively if we have open access to information and the knowledge generated therefrom. In my opinion, the genesis of the substantial national concern with the draft Executive Order and with reduced access to information is the <u>information-knowledge-power triad</u>.

Several weeks ago I became aware of the development of a revised Executive Order which would replace 12065. After reviewing a draft of that new order, I became acutely aware of a dramatic change in the tone of the order, and of its fundamental hypothesis. The draft reverses trends well established by the three previous Executive Orders.

The record of the Congress concerning these vitally important matters has been well established (Ref. 21-26). For example, the Committee on Governmental Operations held a hearing on March 11, 1982, that provides substantial and well articulated testimonies about the crucial issues related to the draft Executive Order. All the testimony is important to understand; however, I would like to note particularly that of Professor Mary M. Cheh (Ref. 2). She speaks insightfully about the problems that grow out of this new draft. She discusses effectively the dangers of erring in the direction of secrecy. Further, the "Congressional Record" is filled with many excellent examples of problems regarding access to national security information (Ref. 21-26).

If one could be assured that national security information were to be classified only in those cases which clearly and unquestionably threaten our national security, and if there were a clear, common understanding of "national security", we would undoubtedly not be here today. It is human interpretation that complicates this whole matter. Some individuals feel that new

and substantial restrictions are required to protect the security of our nation. Others feel that openness is the central ingredient to national growth, development and even survival. These are tough and maybe even unanswerable questions. Therefore, Mr. Chairmen and Committee members, I would like to propose a relatively simple, but, I hope, constructive suggestion.

III. A Proposal

We engaged in a life threatening war about 40 years ago. During that time, the role and importance of national security information became imminently clear. In the world of nations we were young and in many ways extraordinarily naive concerning the relationship between information and national security. As a consequence, laws were passed (i.e. National Security Act of 1947) and a first Executive Order on National Security Information was written. Further, several pieces of legislation have been enacted, i.e., the Invention Secrecy Act of 1951, the Atomic Energy Act of 1954, the Arms Export Control Act of 1976, the Export Administration Act of 1979, the International Traffic in Arms Regulation, the Freedom of Information Act, and others. These have been the Government's response to a need to effectively control information, therefore knowledge, in our best interest. I suggest that each of these acts, regulations, and Executive Orders (Ref. 27-30) was in direct response to a specific problem deemed vital to our national security.

Since World War II, those items of information vital to our national security and those items of information vital to the growth and vitality of our nation have become so intertwined that it is now almost impossible to separate them. The distinction between them is almost imperceptible. The simplicity inherent in a World War II intelligence problem is no longer present in a world filled with high technology, computer systems, complex manufacturing systems, microelectronics, and the like. In short, information which is vital to our national security is also vital throughout the industries and institutions of the country.

What is at stake, in my opinion, is an undergirding assumption about our nation and its future. It is out of this perspective that I believe it is time for us to pause, not to issue new Executive Orders or pass new laws to control security information, but to place the highest priority on a far-reaching national assessment of the role that information has in our nation's security and will have in the future vitality of this democracy. I suggest the Congress, in concert with the President of the United States, establish a National Commission to comprehensively address, in a timely fashion, the problems we are discussing here today. I suggest that the Commission examine the various laws, orders, and acts which bear upon these issues, and draw out the essential elements which truly effect our national security. Only after a careful analysis will we be able to be sure that regulations protect that which needs protection,

leaving the greatest possible latitude for intellectual, economic and social development. A thoughtful and comprehensive assessment will provide the foundations that will determine the health and strength of our country for generations to come. Such a Commission would necessarily be composed of representatives of Congress, military planners, members of the National Security community, leaders of industry and government, representatives of the academic world, the free press and other equally important sectors of our society. The timing is right, and the needs are clear; many sectors of our society are vitally concerned that these issues be fully addressed and resolved. In my opinion, the concern which has been so strongly expressed during the past weeks suggests siezing an opportunity to bring wholeness to our national security information problems instead of the piecemeal approach of the past four decades. The work of such a Commission should lead to regulations which could effectively address our national security needs while neither undermining the fundamental precepts of our democracy nor inhibiting the growth of science and technology. In my opinion this should be given the highest priority of government and should be addressed immediately.

I am grateful for the opportunity to meet and talk with you today. As I have prepared for this session, I have been increasingly overwhelmed by the fundamental nature of the discussions in which we are engaged. I have had the opportunity to appear before Congress on many occasions to address many specific topics. None have had a higher magnitude of importance, than the one you are addressing today. It is my sincere hope that the collective wisdom of Congress can be brought to bear in such a way that we address these issues directly and comprehensively, and that out of these hearings and the actions that I hope you and your colleagues take, our nation will bring unity and a rational understanding to the control of national security information and its subsequent impact on the knowledge base of our country.

Thank you.

Best Available Copy

REFERENCES

1. Carey, W.D. Testimony before Subcommittee on Science, Research and Technology Hearings on the National Science Foundation. February 23, 1982.

2. Cheh, M.M. Testimony before The Government Information and Individual Rights Subcommittee of the Committee on Government Operations House of Representatives, Congress of the United States on A Proposed New Executive Order on Security Classification. March 10, 1982.

3. Adler, A.R. and Halperin, M.H. Statement Before the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations on the Reagan Administration Proposal to Revise the Executive Order on National Security Information. March 10, 1982.

4. Nelson, A.K. Statement Before the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations. March 10, 1982.

5. Schieffer, R. Testimony on Behalf of the Society of Professional Journalists, Sigma Delta Chi before the House Subcommittee on Government Information and Individual Rights. March 10, 1982.

6. Rowe, C.S. Statement representing the American Newspaper Publishers Association and American Society of Newspaper Editors before the Subcommittee on Government Information and Individual Rights Committee on Government Operations concerning Executive Order on Classification. March 10, 1982.

7. Garcia, O.N., President, IEEE Computer Society, letter, March 7, 1982.

8. Carey, W.D. Science (editorial). 6 November 1981, Volume 214, Number 4521.

9. Kolata, G. Science. 5 February 1982. Vol. 215. P. 636.

10. Sokal, M.M. Science. Vol. 215. P. 1182.

11. Kolata, G. Science. 5 February 1982. Vol. 215. P. 638.

12. Petersik, J.T. Science. 19 February 1982. Vol. 215. P. 912.

13. Kolata, G.B. Science. 6 November 1981. Vol. 214. P. 646.

14. Kolata, G. Science. 12 March 1982. Vol. 215. P. 1379.

Best Available Copy

15. Science 82, Special Report. April, 1982. P. 12.

16. The Washington Post editorial. "Secrecy, Security and Science." January 18, 1982.

17. Chemical and Engineering News editorial. "The Flow of Scientific Information." November 23, 1981. P. 3.

18. Broad, W.J. Science. 26 March 1982. Vol. 215. P. 1591.

19. Chemical and Engineering News. 8 March 1982. P. 7.

20. Chemical and Engineering News. 15 March 1982. P. 6.

21. Congressional Record. November 10, 1981. P. E5225

22. Congressional Record. January 25, 1982. P. H18.

23. Congressional Record. February 11, 1982. P. S769.

24. Congressional Record. February 22, 1982. P. E426.

25. Congressional Record. February 25, 1982. P. H511.

26. Congressional Record. March 1, 1982. P. S1298.

27. Executive Order 10290 (Truman) 16 Federal Register 9795. September 24, 1952.

28. Executive Order 10501 (Eisenhower) 18 Federal Register 7049. November 5, 1953.

29. Executive Order 11652 (Nixon) 37 Federal Register. March 10, 1972.

30. Executive Order 12065 (Carter) 3 Congressional Federal Register 190. 1979.

Mr. GORE. Thank you very much for an excellent statement.

I would like to hear next from Dr. Edward Gerjuoy from the University of Pittsburgh, and representing the American Physical Society.

Dr. Gerjuoy, welcome.

Dr. GERJUOY. As you were informed, I am testifying today as a representative of the American Physical Society, in my capacity as immediate past chairman of the society's panel on public affairs.

The American Physical Society, with over 30,000 members, is the largest organization of professionally active physicists in the world. The society's objective, explicitly stated in its constitution, is the advancement and diffusion of the knowledge of physics. This object is furthered in very large part through the meetings and publications the society maintains. Each year the society conducts a variety of meetings with a total attendance this past year of about 20,000. The society also publishes a number of physics journals, including the Physical Review, probably the most widely read and most prestigious physics journal in the world.

For these reasons, but also because the society and its members are genuinely devoted to and have worked for this Nation's welfare, the American Physical Society has been concerned about recent attempts to restrict the flow of scientific information. The society has formally expressed its views on proposed export con-

Best Available Copy

trols in a letter to George Keyworth, Director of the Office of Science and Technology Policy. However, the society has not had the opportunity to formulate precisely its views on the latest revisions to President Reagan's draft Executive Order on National Security Information. Therefore, my presentation today of the American Physical Society views concentrates on export control issues.

I am confident, however, that the society's views on the general subject of the impact of national security considerations on science and technology, when formulated, will be well indicated by the overall tenor of my remarks on the more specific export control problem. I am equally confident that my testimony will be supported by a very large majority of the members of the American Physical Society.

Now, neither the American Physical Society nor I adhere to the doctrinaire view that there should be no export controls. Of course, Government controls on exports of military weapons, or their blueprints, are needful to our national security. But weapons are things. The community of American physicists accepts the need for export controls on things—equipment, commodities, devices—that have the "capacity for substantial utility in the conduct of military operations."

In the past 2 years, however, the Federal Government has been attempting to extend its export controls from well-defined categories of things to very broadly and correspondingly vaguely defined categories of scientific and technical information, termed "technical data" in the export regulations.

These regulations also define "export" very broadly. The present regulations say that export of technical data may occur through "oral exchanges of information in the United States or abroad, or through the application to situations abroad of personal knowledge or technical experience acquired in the United States."

In other words, the Government apparently is proposing to create a vast new category of unclassified yet somehow restricted information, open to all American citizens, but closed to foreigners without Federal authorization. Forbidden exports would include oral as well as written communications to foreign nationals.

The American Physical Society does not quarrel with the Government's objective—preventing the spread of high technology which could make a significant contribution to the military potential of unfriendly nations. However, the society does question whether the Government's present approach to this objective can achieve its goal without impeding the continued progress of American science and thereby counterproductively weakening rather than strengthening this Nation.

In particular, the control measures will very likely greatly hamper the free exchange of scientific information between our own nationals without greatly diminishing the flow of such information to the Soviet Union. The Soviet Union trades with and receives technical data from Western Europe and Japan, which together have a very significant scientific and technological base. But the hampering of scientific communication between Americans may very greatly damage American science, which has flourished in our open society.

In the nearly 40 years since World War II, Soviet science, like Soviet society, has been closely controlled. Nevertheless, by any reasonable criterion, the United States continues to be scientifically and technologically ahead of the Soviet Union. The very reason the Government gives for the proposed export controls, that the Russians desperately seek our science and technology, is evidence that we have kept ahead.

Moreover, it is very hard to know what information should be restricted. For example, the paper that describes how a laser might be built, published in the Physical Review in 1958, and which eventually earned its Bell Laboratories author a Nobel prize, almost certainly would not have been controlled at the time. Nobody visualized what a laser could do, and most people thought that actually constructing a working laser would be quite difficult, if not impossible. Nevertheless, 1½ years later, a working laser was constructed by a Hughes Aircraft group in California, not the original Bell Labs group, mind you, but by a group which was hardly known to the Bell Labs group.

So I ask the question, Isn't it likely that keeping the 1958 Bell Labs paper secret, and hoping the Russians wouldn't think of a workable laser design, would have been a poorer guarantee of our staying ahead than the course we actually took; namely, letting the design be published and relying on the rapid response of our open scientific society to keep us in the forefront should lasers prove to be militarily important, as they indeed turned out to be?

Therefore, one has to ask, Why tamper with scientific practices that have kept us ahead? Why risk the duplication of effort, the false starts that our present open system of scientific communication helps to avoid? Why risk the alienation, the loss of pleasure in doing research, the migration of scientists to other endeavors, that an extensive system of bureaucratic controls on publications might foster on American scientists? Why risk making it less likely than even now that American high school graduates will be impelled to go into science instead of going into other areas, as they presently seem to want to do?

The administration should agree that it bears the burden of proof that the controls it proposes are necessary, in general and in specific areas. The American Physical Society especially stresses that at the very least, if the administration continues to insist that it must have new regulations controlling the transfer of technical information, then these regulations should be prepared in continuous consultation with representatives of the affected scientific, educational and industrial communities, and not just by Government agencies alone.

The Government should also recognize that the American scientific community is as patriotically dedicated to our American way of life and to keeping the United States secure against military threats as any segment of this Nation's society. Therefore, the administration should pay very serious heed to the scientific community's knowledgeable warnings about the dangers to our science inherent in the newly proposed controls, and likewise should heed the informed warnings of America's equally patriotic and dedicated educational and industrial research communities about the dangers posed to them.

Now, before closing, I want to point out that my testimony deliberately has made no reference to the possibilities that the administration's proposed information controls are unconstitutional or may jeopardize the postures the United States has adopted concerning violations of human rights by the Soviet Union. I am not unaware of or indifferent to these possibilities, but I prefer to leave them to other witnesses. My case is that the proposed information controls are unwise and will be harmful to the United States irrespective of constitutional and human rights considerations, and this is the only case I have tried to make.

I add, after hearing the previous testimony, that evidently the point of view I have espoused is very close to Dr. Rosenzweig's, and if I had to summarize my testimony in a few words, I would say "If it's not broken, don't fix it."

The American Physical Society and I thank you for this opportunity to testify.

[The prepared statement of Dr. Gerjuoy follows:]

The American Physical Society
335 EAST 45 STREET, NEW YORK, NEW YORK 10017 • (212) 682-7341

PRESIDENT
MAURICE GOLDHABER
BROOKHAVEN NATIONAL LABORATORY

PRESIDENT ELECT
ROBERT E. MARSHAK
VIRGINIA POLYTECHNIC INSTITUTE

VICE PRESIDENT
MILDRED S. DRESSELHAUS
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

EXECUTIVE SECRETARY
W. W. HAVENS, JR.
COLUMBIA UNIVERSITY

TREASURER
JOSEPH A. BURTON
BELL LABORATORIES (RETIRED)

Testimony Presented to the Joint Hearings:

Investigations and Oversight Subcommittee
and Science, Research and Technology Subcommittee
of the House Committee on Science and Technology

on the Impact of National Security Considerations on Science and Technology

Edward Gerjuoy
March 29, 1982

Best Available Copy

97-341 O - 82 - 9

My name is Edward Gerjuoy. My present employment, as an administrative law judge, reflects the fact that I am an attorney as well as a physicist; I am a member of the Commonwealth of Pennsylvania Environmental Hearing Board, on leave from my post as a tenured professor of physics at the University of Pittsburgh. However, most of my professional life since receiving my physics Ph.D. degree in 1942 has been spent in university physics teaching and research, although I also worked full time in industry for six years and have been a consultant to numerous industrial and government research establishments.

I am testifying today as a representative of the Americal Physical Society, in my capacity as immediate past chairman of the Society's Panel on Public Affairs. The American Physical Society, with over 30,000 members, is the largest organization of professionally active physicists in the world. The Society's objective, explicitly stated in its constitution, is the advancement and diffusion of the knowledge of physics. This objective is furthered, in very large part, through the meetings and publications the Society maintains. Each year the Society conducts four general meetings, plus a considerably larger number of more specialized meetings, with a total attendance this past year of about 20,000. The Society also publishes a number of physics journals, including the Physical Review, probably the most widely read and most prestigious physics journal in the world. Last year these publications contained about 5,000 articles, totaling about 40,000 densely packed pages, much like the Congressional Record in size and format. These articles were contributed from every continent, including Iron Curtain countries, and every published article had to be approved by at least one of some 10,000 specialist referees.

Best Available Copy

For these reasons, but also because the Society and its members are genuinely devoted to this nation's welfare, the American Physical Society has been concerned about recent attempts to restrict the flow of scientific information. These concerns, and the Society's views, have been espressed formally in a letter sent February 9, 1982 by Maurice Goldhaber, President of the American Physical Society, to George Keyworth, Director of the Office of Science and Technology Policy. This letter, which is attached to my testimony, discusses the Administration's intended revisions of this nation's export regulations, specifically the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). The Society has not had the opportunity to formulate precisely its views on the latest revisions to President Reagan's draft Executive Order on National Security Information. Therefore my presentation of American Physical Society views concentrates on export control issues.

I am confident, however, that the Society's views on the general subject of the Impact of National Security Considerations on Science and Technology, when formulated, will be well indicated by the overall tenor of my remarks on the more specific export control problem. I am equally confident that my testimony will be supported by a very large majority of the members of the American Physical Society. I add that my testimony is wholly consistent with the remarks concerning attempts to restrict scientific communication made by Arthur Schawlow, 1981 Nobel Laureate in physics and immediate past president of the American Physical Society, in testimony delivered February 25, 1982 to this Committee of Science and Technology. My testimony also is consistent with the editorial "Unwise Export Controls can Hurt", which appeared in the October issue of the very widely read American Institute of Physics semi-technical publication Physics Today; as the Committee knows, this editorial, written by me, was inserted in the Congressional Record of January 25, 1982,

Best Available Copy

p. H-19, by Congressman George Brown.

As these earlier statements clearly indicate, neither the American Physical Society nor I adhere to the doctrinaire view that there should be no export controls. Of course government controls on exports of military weapons, or their blueprints, are needful to our national security. I was outraged--and I feel certain that just about every physicist in this nation was outraged--to learn (New York Times, November 20, 1981) that an attempt had been made to evade export licensing requirements in a shipment to Pakistan of 5000 pounds of zirconium, used in nuclear fuel element manufacture. No doubt many physicists will disagree with the government about controls on various individual items, but on the whole the community of American physicists accepts the need for export controls on <u>things</u>--equipment, commodities, devices--that have the "capacity for substantial utility in the conduct of military operations" (quoting from the definition of "significant military equipment" in §121.313(a) of the proposed revised ITAR Regulations, published for public comment in the Federal Register, December 19, 1980, pp. 83970ff.)

In the past two years, however, the federal government has been attempting to extend its export controls from well-defined categories of <u>things</u> to very broadly and correspondingly vaguely defined categories of scientific and technical <u>information</u>, termed "technical data" in the export regulations. For example, §379.1(a) of the EAR presently in effect defines technical data which may require control as: "information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials". Section 379.1(b) says export of technical data may occur through "Oral exchanges of information in the United States or abroad", or through "The application to situations abroad of personal knowledge or technical experience acquired in the United States".

It is true that under the EAR much technical data can be exported without the formality of obtaining an export license from the Commerce Department; but it also is true that Section 5(d) of the Export Administration Act of 1979 requires the Secretary of Defense to develop a list of militarily critical technologies, whose technical data (defined as above) almost surely will be subject to control. Moreover, a preliminary list of energy related militarily critical technologies, prepared by the Department of Energy and published in the Federal Register, October 1, 1980, pp. 65152ff is itself very broad.

Indeed, it would be extremely difficult to find an experiment published in a recent issue of the Physical Review which did not make use of some equipment listed in the aforementioned October 1, 1980 Federal Register under the heading "keystone hardware", defined as the "unique hardware components that are necessary for the effective development or application of" the various militarily critical technologies. For example, under "diagnostic technology", just one of the more than 140 critical technologies listed, the "keystone hardware" includes: streak cameras, neutron detectors, gamma detectors, X-ray detectors, fast analog circuitry, fast oscilloscope (picosecond sweep), computers, X-ray transmission equipment, neutron radiography equipment, microwave acoustic microscopy equipment, spectroscopy equipment, magnetic field measuring equipment, Thomson scattering equipment, interferometry equipment, pin probes, flash X-ray probes and diagnostic lasers.

In other words, the government apparently is proposing to create a vast new category of unclassified yet restricted information, open to all American citizens but closed to foreigners without federal authorization. Forbidden exports would include oral as well as written communications to foreign nationals. With both exports and controllable information so broadly categorized, effective enforcement of export controls seems impossible without

Best Available Copy

expensive and stultifying expansions of paperwork and bureaucracies, along with measures that will greatly hamper the free exchange of scientific information between our own nationals, not merely between American citizens and foreigners. The effects on our universities, professional societies and industrial research laboratories will be profound, and very likely highly deleterious. For instance, universities seemingly will have to restrict either the attendance or the content of many courses and colloquia, and physics professors will find it almost impossible to work with foreign pre-doctoral or postdoctoral students in their laboratories, because frontier experimental physics research almost inevitably is at the cutting edge of important new technologies. Correspondingly, as we have heard Admiral Inman warn at the January, 1982 national meeting of the American Association for the Advancement of Science, professional organizations like the American Physical Society, who sponsor many of this nation's major scientific journals, may have to modify their heretofore highly successful publication policies.

The American Physical Society's position on the government's recent attempts to control the export of technical data now can be simply stated. The Society does not quarrel with the government's objective—preventing the spread of high technology which could make a significant contribution to the military potential of unfriendly nations. However, the Society does question whether the government's present approach to this objective can achieve its goal without impeding the continued progress of American science and thereby counterproductively weakening rather than strengthening this nation.

The Society especially wishes to emphasize its view that if increased export controls on scientific and technological information are demonstrably necessary for the welfare and security of this nation, the needed regulations should be formulated and implemented in consultation with the officers of scientific societies, university administrators and productive industrial and

Best Available Copy

academic scientists, able to appreciate the risks unwise export controls can pose to our scientific organizations, educational institutions and high-technology industries. Because the government's attempts during the past few years to enforce the new approach to export controls have not shown much appreciation of these risks, the Society is gratified that the Defense Department recently has instituted a DOD/University Forum, composed of high-ranking DOD officials and university administrators, charged with the task of examining export controls and other national security measures affecting university scientific research and education.

The American Physical Society believes that this Forum, which had its first meeting February 24, 1982, should be broadened to include scientific society representatives and productive scientists, and recommends that other government agencies, particularly the State and Commerce Departments responsible for the ITAR and EAR respectively, follow the Defense Department's lead. I do not know if this matter can be dealt with legislatively, but if so I hope the Science and Technology Committee will agree it is desirable that national security regulations affecting science and technology be prepared in active consultation with members of the affected scientific, educational and industrial communities, rather than limiting these communities to preparing comments on solely agency-produced regulations which, by the time they are promulgated for comment, already may be nearly set in concrete.

Now, if I may, I would like to make some more personal remarks, in elaboration of the foregoing rather formal exposition of the American Physical Society's views. In the nearly forty years since the Second World War Soviet science, like Soviet society, has been closely controlled, with the West permitted to glimpse only what the KGB is willing to release. During the same period our science, like our society, has been open to anyone's glance, except for a

Best Available Copy

limited number of classified military research projects. Nevertheless, by any criterion I can think of--Nobel Prizes, numbers of scientific papers published, important inventions, manufacture of high-technology items, new medicines, any measure that's at all sensible--the United States continues to be way ahead of the Russians, although inevitably here and there one finds scientific subfields where they compete favorably. The very reason the government gives for the proposed export controls, that there is a flow of technical information from us to them, which the Russians eagerly foster, is evidence that we have kept ahead. Nor is it convincing to argue that the Russians are behind because they started way behind. In the first place, forty years is an immensely long time at the pace with which modern science progresses. Secondly, Germany and Japan, whose economies also were demolished during World War Two, have become far greater challenges to our technological superiority than the Soviet Union.

Furthermore, it is not surprising that our open society has stayed scientifically and technologically ahead of the Russian closed society; it would have been surprising if the advantage had gone the other way. It is difficult for modern science to flourish without open communication and publication, which enable a researcher to be stimulated by new ideas from specialists in diverse disciplines and to stimulate them in return. Most of us are not Leonardo da Vincis; Leonardo himself would have had a hard time mastering more than a few of today's scientific disciplines. Today's scientists have to rely on the accumulated experience and ingenuity of other scientists. However, without widely advertised open meetings, without widely circulated scientific journals, it is impossible to learn rapidly about scientific progress elsewhere or--of equal importance to most researchers--to discover whom to consult for needed specialized technical information. If I may use a physicist's simile: adding impediments to scientific communication is like

Best Available Copy

adding friction; the result is more wasted energy and a slowing of scientific progress.

Illustrations from the history of modern science, bearing out the import of the immediately preceding remarks, are not hard to find. For instance, Arthur Schawlow, in the testimony I have cited, points out that in December 1958, when he and Charles Townes first published their Physical Review paper describing how a laser might be built, most people thought that actually constructing a working laser would be quite difficult if not impossible. Nevertheless, an operating laser was announced no later than mid 1960, by Theodore Maiman at the Hughes Aircraft Company's research laboratories in Malibu, California. Before the end of 1960, no fewer than five different kinds of operating lasers had been demonstrated (A. Schawlow, "Masers and Lasers", IEEE Transactions on Electron Devices, vol. ED-23, July 1976, p. 773). The laser developed by Schawlow's own group at Bell Laboratories was one of the last of these five to succeed, and Schawlow himself describes how--after writing his December 1958 paper--his efforts to construct an operating laser were only desultory until Maiman showed it indeed could be done (Schawlow, IEEE paper, ibid).

It is important to recognize that unless this nation intends to set up an enormously cumbersome system for controlling the availability of unclassified scientific publications at libraries, in faculty offices, even at the printer's, export controls of the sort the Administration presently envisages could not have kept the Schawlow and Townes 1958 paper out of Russian hands, once it had been published in the Physical Review. This conclusion, which appears to be obvious, also was reached in an excellent study which I call to this Committee's attention, prepared by the Department of Commerce for the Congress, pursuant to Section 120 of the Export Administration Amendments of 1977, Public Law No. 95-52. This study, titled "Exports of Technical Data by Publication or

Best Available Copy

Other Means of Public Dissemination", and embodied as Appendix D of what appears to be a 1978 Semiannual Report under the Export Administration Act, states: "Because it is virtually impossible to prevent the export of information publicly available within the United States, the report assumes that the public availability of technical data within the United States is tantamount to their export." Elsewhete the same study asserts:

> "The practical problems associated with a post-publication control system would be enormous. Even if its scope were limited to the review of certain types of media, its operation would involve exorbitant administrative costs.
>
> The effectiveness of such a system is extremely doubtful. Efforts to remove sensitive technical data from public access might decrease the likelihood of their subsequent export, but it would be virtually impossible to determine whether the data had been exported during the period of public availability prior to control by the U.S. Government or to be sure that the data had been removed from future public access. The impact on scientific development and research would, of course, be adverse because of the constraint on the exchange of information relating to scientific and technical research".

In effect, therefore, the Schawlow-Townes 1958 paper on the possible design of a laser could have been kept from the Russians only by severely limiting its distribution within the United States, in other words only by classifying it. However, it also is important to recognize that even if President Reagan's draft Executive Order on National Security Information had been in force in 1958, the Schawlow-Townes paper almost certainly would have remained unclassified, as "basic scientific research not clearly related to national security". At the time the paper was published there was little confidence that a laser could be built, and hardly an inkling of what lasers can do.

Nonetheless, it may be of interest to raise the hypothetical question: Would classifying the Schawlow-Thomas paper in 1958 have enhanced the security of the United States? The answer to this question is highly speculative, of course, but it does seem doubtful that a "yes" answer can be correct. The rapid development by American physicists of an operating laser, made possible by the wide circulation of the Schawlow-Townes paper, enabled the United States, not the Soviet Union, to take the

Best Available Copy

lead in many important new technologies, including retinal surgery and computer chip manufacture. Schawlow's testimony observes that estimated 1981 worldwide expenditures on lasers amount to $1.27 billion dollars, and that the laser industry makes a substantial contribution to this country's export trade. True, lasers have military applications as well, which we have taken advantage of, but which the Russians undoubtedly can use against us. On the other hand, surely we are glad that the first lasers were built by Americans, not Russians. It seems unlikely that keeping the Schawlow-Townes paper secret, and hoping the Russians wouldn't think of a workable laser design, would have been a better guarantee of our first constructing an operating laser than the course we actually took, namely letting the Schawlow-Townes paper be published in the Physical Review for everyone to see (including Russians in Moscow, but including also Hughes Aircraft physicists in Malibu with whom Schawlow had little contact), and then relying on the rapid response of our open scientific community to keep us in the forefront of any useful implications of the Schawlow-Townes work. Actually a quite probable consequence of our keeping the Schawlow-Townes paper secret would have been the independent invention of the laser by a Western European or Japanese scientist, who would have published his results for both Russian and American scientists to see.

Because of the international character of science, American scientists are better acquainted than most of their compatriots with the deficiencies of the Soviet system. I have been in the Soviet Union four times, including spending a month as the Lebedev Institute, the prestigious Moscow laboratory where Andrei Sakharov worked before he was exiled to Gorky. I have seen at first hand the inefficiencies and petty aggravations imposed on Soviet scientists. I also have seen the irritation and disaffection in the eyes of a Soviet colleague as he explained that any paper emanating from his laboratory, however innocent of possible application, had to receive KGB approval before it could be published.

Does the government imagine American scientists would or should take more kindly than their Soviet counterparts to similar requirements for pre-publication

Best Available Copy

review? I know that in his now-famous talk Admiral Inman stated:

> "I think it should also be pointed out that scientists' blanket claims of scientific freedom are somewhat disingenuous in light of the arrangements that academicians routinely make with private, corporate sources of funding. For example, academicians do not seem to have any serious difficulty with restrictions on publications that arise from a corporate concern for trade secret protection. The strong negative reaction from some scientists, over the issue of protecting certain technical information for national security reasons, seems to be based largely on the fact that the federal government, rather than a corporation, is the source of the restriction. Yet this would presume that the corporate, commercial interests somehow rise to a higher level than do national security concerns. I could not disagree more strongly".

I am not acquainted with any scientists who think corporate commercial interests are more important than national security concerns. I certainly don't think so. But surely Admiral Inman and the government must recognize that the scientific community's willingness to accept publication restrictions on voluntarily contracted corporate-funded research does not require a willingness to accept without protest an involuntarily imposed all-embracing system of publication controls, which can be disobeyed only at a risk of criminal penalties, not just losing a consulting contract.

Indeed, limiting the interchange of information between American scientists is not the only way to slow up American science. The disaffection and loss of research time produced by requiring American scientists to interact extensively with a scientifically less well educated bureaucracy, such as the bureaucracy needed to administer the government's proposed export controls, also can have significant adverse results for American science. The paralyzing effects of disaffection on a research scientist's motivation, which correlates highly with research productivity, should not be underestimated, and is attested to by the enormous number of Soviet scientists whose disaffection has led them to give up their (by Soviet standards) well paid jobs and seek emigration, even at the risk of imprisonment.

I am neither suggesting nor expecting that disaffection with export controls is going to cause American scientists to emigrate, and if they were to emigrate they certainly would not go to the Soviet Union; the American scientific community is not

Copy

Best Available Copy

stupid. But there is the very real danger that imposition of bureaucratic controls will decrease the satisfactions--the esprit de corps, the pleasures of freely communicating with fellow scientists, the thrill of getting a fresh idea from reading a paper and thereby beating the entire world's competition on a problem--that keep scientists in research and university teaching instead of finding more lucrative and less demanding jobs, which most scientists probably could do. Failure to keep scientists in active research, failure to train enough new scientists to fill vacancies that open up, are sure-fire mechanisms for the United States to fall scientifically and technologically behind its enemies. We already are finding it difficult to train enough native American Ph.D's to staff our universities. In 1979, almost half the Ph.D's granted in engineering in American universities went to foreigners (Industrial Research and Development, March 1982, p. 59); in 1980, ten percent of all faculty positions at U.S. engineering colleges were unfilled (Science, December 11, 1981, p. 1223). In weighing the pros and cons of its proposed information control measures, the government must not ignore the likely impact of these measures on the ways in which American researchers and university professors--along with American high school students--will regard a scientific career.

As a matter of fact, the history of the government's still very limited attempts to enforce its new approach to export controls does not suggest the enforcing bureaucracy will be able to avoid irritating, if not repelling, the scientists with whom it comes in contact. The first indication of the new approach seems to have occurred toward the end of the Carter administration, with a Commerce Department intervention into an International Conference on Bubble Memory, organized by the American Vacuum Society at Santa Barbara, California in February 1980. About a week before the conference was scheduled to open, the president of the Vacuum Society, which is a member society of the American Institute of Physics, received a letter from the Commerce Department saying:

> It has come to my attention that presencations to be made at the Conference may fall within the scope of Part 379 (Technical Data) of the U.S. Export Regulations (copy enclosed). Under Section

Best Available Copy

> 379.1(b) oral exchanges of information in the U.S. with foreign nationals constitute the export of technical data. Under Section 379.4(f), a validated license from the Office of Export Administration would be required prior to export of such technical data of Eastern European destinations, among others...
>
> You are invited to submit to the Office of Export Administration a request for an advisory letter so that we may make a definitive determination as to what restrictions govern the subject matter of the Conference. The request should include submission of copies of the presentations to be made, sources of the information contained in the presentations, and whether the information is proprietary in nature or in the public domain.

Anybody who ever has organized a Conference, scientific or otherwise, will immediately realize that the Conference organizers couldn't possibly have furnished the information requested by Commerce. Leaving aside the fact that the Conference organizers were given only a week to comply, the fact remains that the information requested simply wasn't known to the recipients of the Commerce letter. In any Conference I've been to, people frequently speak off the cuff. Sometimes they furnish manuscripts in advance, but at least as often they don't. Conferences frequently do require that abstracts be submitted in advance, but a delivered talk often departs considerably from the advance abstract. And anyway, who can know what a speaker will say in response to a question, and what conference organizer can tell whether the speaker will have adequate sources for his assertions or whether the information to be presented is in the public domain? Conference organizers simply have to expect that speakers will use good judgment. For example, this Santa Barbara Conference was totally unclassified, so the organizers naturally assumed that no speaker would be imparting classified information. But, in such an unclassified conference, if a speaker were to give away classified information, the Conference organizer has to take the view that it's the speaker's responsibility, not the organizer's. If an organizer is going to be held responsible for improprieties by any one of his speakers, no one will be willing to organize a Conference, which often involves a lot of extra work for an al-

Best Available Copy

ready harassed researcher, without any special glory believe me, I've been there.

John Vossen, the Vacuum Society President, tried to explain all this to the Commerce Department, but it was no go. He was informed that the Conference could not proceed unless Eastern bloc participants were disinvited, and that failure to obey the Commerce Department's requirements was punishable by a $10,000 fine, ten years in prison, and an additional fine of 5 times the value of any equipment seen or demonstrated. So the Soviet bloc participants indeed were disinvited, and the other foreign participants were required to sign a letter of assurance that information obtained at the Conference would not be divulged to Eastern bloc nationals. The Commerce Department apparently was not concerned that such a requirement might make it awkward for American scientific societies to invite distinguished foreign scientists to our conferences or that such scientists, if invited, might refuse to accept a Commerce-imposed censorship of their future scientific contacts.

This last remark raises a fairly evident matter that I have not mentioned heretofore. Although the United States still is ahead of any single country, the combined talents of Japan and the Western European democracies do offer a very significant scientific and technological challenge to the United States. There is nothing in the news we read every day, for instance in the news about the Administration's efforts to get our Western allies to reduce their trade with the Soviet Union, to suggest that these allies will agree to restrict the export of technical data to the Eastern bloc. But unless our allies--who trade quite freely with us and have strong intrinsic strengths of their own--do control their technical data exports, of what avail is it for us to impose controls? The most likely result of our unilateral imposition of export controls would be to heap restrictions on communications between our scientists and Western scientists onto the already discussed anticipated restrictions on communications among our own American scientists, thereby further weakening American science without seriously hindering the Soviet Union's access to Western technical data.

Best Available Copy

Let me sum up my personal views. For reasons like the foregoing, I--and most scientists--cannot fathom why the government thinks our national security will be advanced by instituting export controls on technical data and increasing the classification of such information. I am aware that those reasons do not prove the government's approach is wrong; one doesn't need to be a scientist to appreciate the fact that I have been unscientifically examining a political question, to which no provably correct answer can be given. But I also am aware, and I hope the government is aware, that the American scientific community is as patriotically dedicated to our American way of life, and to keeping the United States secure against military threats, as any segment of this nation's society. The Administration should pay very serious heed to the scientific community's knowledgeable warnings about the dangers to our science inherent in the newly proposed controls, and likewise should heed the informed warnings of America's equally patriotic dedicated educational and industrial research communities about the dangers posed to them.

Above all, the Administration should recognize it is proposing to tamper with scientific practices which have kept us ahead; therefore the Administration should agree it bears the burden of proof that the proposed controls are necessary, in general and in specific cases. At the very least, if the Administration continues to insist it must have new regulations controlling the transfer of technical information, these regulations should be prepared in continuous consultation with representatives of the affected scientific, educational and industrial communities.

Before closing I want to point our that my testimony deliberately has made no reference to the possibilities that the Administration's proposed information controls are unconstitutional, or may jeopardize the postures the United States has adopted concerning violations of human rights by the Soviet Union. I am not unaware of or indifferent to these possibilities, but prefer to leave them to other witnesses. My case is that the proposed information controls are unwise and will be harmful to

Best Available Copy

the United States irrespective of constitutional and human rights considerations, and this is the only case I have tried to make. Nevertheless, I feel constrained to mention that on January 31, 1980, Professor Herman Feshbach of MIT, then President of the American Physical Society, testified to this Committee about the American Physical Society's activities on behalf of the human rights of physicists everywhere, including Andrei Sakharov, Yuri Orlov and some 60 other physicists in the Soviet Union. At that time, Professor Feshbach stated:

> "Points of particular concern are unreasonable restrictions on the freedom to attend scientific conferences, on the freedom to publish in scientific journals, on the freedom to have access to scientific literature and unreasonable restrictions on the freedom to pursue their scientific interests and to communicate with other scientists via normal channels including international travel."

It seems noteworthy, and so I note, that these words were spoken by Professor Feshbach less than a month before the previous Administration, with its intervention into the International Conference on Bubble Memory, unveiled its new approach to technical information control.

The American Physical Society and I thank you for this opportunity to testify before you.

Best Available Copy

The American Physical Society
335 EAST 45 STREET, NEW YORK, NEW YORK 10017 • (212) 682-7341

PRESIDENT
MAURICE GOLDHABER
BROOKHAVEN NATIONAL LABORATORY

PRESIDENT ELECT
ROBERT E. MARSHAK
VIRGINIA POLYTECHNIC INSTITUTE

VICE PRESIDENT
MILDRED S. DRESSELHAUS
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

EXECUTIVE SECRETARY
W. W. HAVENS, JR.
COLUMBIA UNIVERSITY

TREASURER
JOSEPH A. BURTON
BELL LABORATORIES (RETIRED)

February 9, 1982

Dr. G. A. Keyworth, Director
Office of Science and Technology Policy
Executive Office of the President
Washington, D. C. 20500

Dear Dr. Keyworth:

I am writing in connection with the Administration's intended revision of this nation's export regulations, specifically the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). This subject has received considerable attention in the news media recently, especially after Admiral Inman's talk at the Washington AAAS meeting in January. The American Physical Society has been concerned about this matter for more than a year, as I believe Bill Havens informed you when he discussed the export control question with you last October.

The APS recognizes that control of some exports is critical to our national security. Unfortunately, many of the Administration's actions and public comments during the past year have caused this Society's governing Council to fear the potentially highly damaging effects on our universities, professional societies and industrial research laboratories that inadvertently could result from unwisely drawn export control regulations. Indeed, unwise export control regulations ultimately may weaken rather than strengthen the United States, and may be capable of effective enforcement only via measures which will threaten the democratic freedoms the nation surely wishes to preserve.

For these reasons, the APS—along with other professional societies and university groups—has been recommending that the Administration prepare the new regulations in active consultation with knowledgeable representatives of academia, industry and professional societies. We are confident that these broad communities, like the APS itself, can identify persons who are willing and able to constructively assist the writing of the new regulations. We understand, and welcome the fact, that the Department of Defense already is taking steps to arrange such consultation and cooperation between the DOD and the academic community.

Best Available Copy

This brings me to the objective of this letter. I hope to enlist your support, in whatever ways you feel appropriate, for the initiation of similar consultative and cooperative steps by the Commerce and State Departments, who are responsible for the actual writing and implementation of the EAR and ITAR, respectively. I assure you that the APS, and many other scientific and educational organizations, will be happy to assist the Administration in developing means for successfully carrying out the consultation and cooperation we recommend.

I should like to add that because the final version of the ITAR now is almost ready for promulgation (we are informed), our recommendation is pertinent primarily to the EAR, whose proposed revisions still are being debated within the Administration. We realize the scientific community probably will have some opportunity to comment on the proposed revisions of the EAR after those revisions are published in the Federal Register, but think damaging effects will be much less likely if this community can make detailed inputs at a time well before the Administration arrives at the admittedly still preliminary language appearing for comment in the Federal Register. Hopefully, our recommended consultation, even if too late to affect the final language of the ITAR, still can be useful in decisions concerning the detailed implementation of the ITAR regulations.

Action on our recommendation is a matter of some urgency, because writing of the proposed EAR is underway. Please feel free to call upon us for any further information you require. We will be happy to meet with you to discuss the subject of this letter, if you so desire.

Sincerely,

Maurice Goldhaber

Maurice Goldhaber
President

Mr. GORE. Thank you for a fine statement. We will hold our questions until the panel is completed.

Dr. John McLucas, president of World Systems Division at Comsat, will go next. And I might note for the record that you have seen this subject from the other side of the fence as Secretary of the Air Force, and we are delighted to have your testimony here today, Dr. McLucas.

Please proceed.

Dr. MCLUCAS. Thank you, Mr. Chairman.

Today we have heard very often the word "balance" as principally a term to indicate the balance between national security interests and private interests of some of the other parties affected by changes in either the laws or regulations affecting transfer of information.

As you have pointed out, I am in something of a balanced position myself. I have 16 years in Government and 20 in private industry.

I am speaking here today on this particular panel as the only spokesman from industry. I should qualify my remarks by saying that I don't think I am a typical industrial spokesman. I'm in the communications business and this is a rather unique business. And so, in order to get the views of industry, I don't think you should rely on me alone.

We are also speaking here today because we are involved in technology transfer outside the United States. Our business among other things includes the export of data, technical data, and consulting services, whereby we assist other nations in taking advan-

tage of space technology and specifically communications satellite technology.

As everyone knows, the communications business involves a lot of information flow, so it seems particularly relevant that we include our kinds of activity in the review which you are conducting.

Mr. GORE. Dr. McLucas, let me just say for the record that we invited the U.S. Chamber of Commerce to come and they expressed the view that they really didn't want to address this directly in this hearing, that it involves the Government and university community predominantly. But we are delighted to have your unique perspective on the issues, so please proceed.

Dr. MCLUCAS. Thank you.

As you all know, Comsat is the U.S. representative designated by statute in both the Intelsat and Inmarsat communication satellite organizations. These are international bodies with in one case 106 members, and the other with somewhat less. But in any case, we deal in our relationships with both Intelsat and Inmarsat as more or less the leading exponent of advanced satellite technology. So far we have been able to maintain the technical lead in advising Intelsat in particular on which direction they should go in future systems. Inmarsat being a younger organization, we have had less history of working with them.

I should point out that while we are dealing in advanced technology, the systems that I am talking about are not military systems, and so we are not dealing in military technology. But in the process of dealing with the U.S. Government with respect to the data which we generate, and want to supply to Intelsat and Inmarsat, we find ourselves in consultation with the Office of Munitions Control and the Department of Commerce.

One point which I meant to mention earlier is that the statute also demands of us that we help the United States to bring modern technology into broader use throughout the world. It is somewhat similar to the Space Act which includes the concept that the United States will not only maintain leadership, but will make the benefits of that technology available to the world at large. The Satellite Act contains some of those same provisions.

In our case, what we are trying to do as we discuss this subject is to balance the legitimate interests of U.S. industry to export their goods and services versus national security objectives of protecting the national interest through preserving certain technology as a U.S. monopoly. I should point out that Comsat has another interest, namely, Comsat Laboratories. We operate the Comsat Laboratories which we think is one of the most advanced communications laboratories in the country, so we are very concerned with any restrictions that might be placed on the activity there.

Now, let me talk for just a minute about some of the problems we have in dealing with the current environment having to do with technology export, and how we think solutions might be found.

First of all, I think that any solution must include much interaction between the Government and the private sector, particularly universities, laboratories, and industry, and if a good dialog is maintained among all these parties, I hope that we will arrive at reasonable answers.

As we have seen the regulations that now exist, and as we have tried to work within them, we are struck by some of the difficulties of dealing in that system. Specifically, we think that it would help if we had a much more simple scheme of reviewing the material which is of concern to the reviewing agencies and more specific lists of critical technology. We have trouble sometimes knowing whether the technology we are talking about falls within or without the proscriptions that have been laid down. We think that we are fairly sophisticated industrial types, and yet we have trouble dealing with the proscriptions, and we suspect that other people in industry have similar difficulty. We believe the rules could be written in a more easily comprehensible form.

Many people might decide not to start down a given road if they knew all the complications that were in the path they are about to embark on. So we propose that simple guidelines be drawn up, that lists of critical technologies be such that the ordinary person could deal with them, and especially we would propose that lists of critical technologies be given frequent updates.

Many of these advanced technologies gradually fall into the public domain, and it is not productive to continue restrictions on items which have already become more or less common knowledge.

Another problem we have is that our requests to release information frequently receive very slow attention. It is not uncommon for us to wait a year or two for answers to some of our requests. If you're participating in a competitive world, a year or two of delay can certainly cool off the ardor of potential customers.

As we have dealt with the individuals in the Government on these subjects, we find that frequently dealing with our problems is a collateral duty for the people in the Government. It seems that if this is an important activity, somehow the Government agencies could be staffed and funded and organized in such a way that this type of review could be conducted much more quickly.

Also, we must submit in each case a fully developed contract about what we propose to do. This means that the review is taking place very late in the game. It means you have sat and negotiated with foreign parties and it comes as a great shock to some of them sometimes to find that in spite of the existence of the negotiated contract there are still further impediments. So it would be better if we could get a tipoff in the beginning that the course we are about to embark on is or is not going to be approved.

Fortunately, because of my previous Government associations, I think I am in a better position than most to explore these matters informally. But I can see that it might be a real impediment to people who aren't so familiar with Washington.

I am struck by the thousands of technical subjects that the Government would have to deal with in order to do a good job of reviewing technology transfer. I don't envy those whose lot it is to police what goes on between the thousands of companies in this country who do export and the potential recipients on the other side. And yet, it seems to me that somehow those lists of technology have to be narrowed down and made much more specific. It is inconceivable that the Government can review all technological activity in the United States and maintain a position on whether a particular technology could be exported.

Now, let me say one more word about our laboratories. The Comsat Labs, as I have said, regards itself as one of the most advanced in satellite communications technology, and we make our advances not only through our internal activity but by keeping in touch with the broad scientific community. It is inconceivable to all of us, I think, to imagine a system whereby we could operate under controls and still make the advances that we do. Although our people are smart, they don't have any corner on knowledge in the satellite field and we learn a lot from others, both through participation in meetings and conferences, and the exchange of private views and all the rest.

Speaking again from the industrial side, I think that U.S. industry finds it very difficult to compete in many high technology areas, and this is rather a contradiction in terms. On the one hand we make rules based on the assumption that we are ahead of everyone else, and at the same time we see a number of our friends, other countries, competing for business overseas which we would like to get. The process demonstrates once again that scientific knowledge and technical acumen is an international enterprise and that we are hard pressed many times to stay ahead of people in other countries in their ability to deliver high technology at a price.

With all the impediments that we have, the competitive disadvantages sometimes of higher labor rates and all the rest, it is no advantage to us have the U.S. Government impose other impediments to U.S. business obtaining overseas customers.

I will just put in a P.S. to Dr. Frank Press' comment about the existence of his committee to explore this whole problem. I happen to serve on that—it's called the Cosepup Committee—which will receive the report of the panel which has been established. I look forward to some considerable enlightenment when that panel has submitted its results.

Thank you, Mr. Chairman.

[The prepared statement of Dr. McLucas follows:]

Statement

of

Dr. John L. McLucas

President, World Systems Division

COMSAT

Before the

Subcommittee on Investigations and Oversight

and the

Subcommittee on Science, Research and Technology

of the

House Committee on Science and Technology

March 29, 1982

Best Available Copy

I am pleased to appear before you today on a subject which has been receiving a good deal of media attention lately. I think I have some insights to provide since in my career I have been "on both sides" of the issue, having served in government posts as well as in industry.

As head of COMSAT's World Systems Division, I have been involved in the policy aspects of technology transfer issues for several years. By statute, COMSAT is the U.S. representative to the International Telecommunications Satellite Organization, a major international organization commonly known as "INTELSAT", which has 106 member countries. INTELSAT is headquartered in Washington, D.C., and has let contracts to many U.S. firms for communication satellites and technical services well in excess of a billion dollars. COMSAT is also the U.S. representative to another international organization known as INMARSAT, the International Maritime Satellite Organization which has already been a source of hardware and study contracts. We have provided technical services to both organizations.

Although COMSAT is not a major defense contractor and it deals principally in technical data rather than hardware, we nonetheless are affected by regulations designed to control the export of sensitive technologies. Since our foreign partners will

Best Available Copy

have access to our spacecraft studies, we have had to file applications with the Office of Munitions Control (OMC) each time we engage in R&D or technical assistance related to satellite facilities for non-domestic use.

A few years ago I served as Secretary of the Air Force in a prior administration. In that position, I saw firsthand how the availability of U.S. technical information to foreign sources could result in improvements in unfriendly military systems. Recent articles by Defense Secretary Caspar Weinberger and others, demonstrating how advanced U.S. technology normally used in benign ways finds its way into foreign military applications, merely reemphasize the lesson I learned during government service. I have concluded that some outflow of technology is part of the price we pay for being a free society. At the same time I realize that it is in our national interest not to encourage the flow of critical technology to our adversaries.

It seems clear that a balance must be struck between the legitimate desires of American business to market its products, technology and services in overseas markets, and the requirements for national security. Let me suggest that in attempting to strike this balance -- to preserve the competitive position of U.S. manufacturers abroad while maintaining national security --

Best Available Copy

several improvements in the current system are necessary. First, Congress and the Executive Branch should strive to keep the technology transfer regulatory scheme as simple as possible. The current Munitions List and Commodities Control List and their accompanying regulations are not helpful to the business community as they are too complicated. Interpretation almost requires a resident government representative on company premises. Guidelines identifying those critical technologies in need of protection should be stated in terms easily comprehended by the business community. Such a reference tool would prove useful to businessmen in considering whether to embark upon a particular overseas project.

Furthermore, Congress, the Executive Branch, industry, and other interested parties must interact frequently to achieve an optimum system. In this regard, the Government must update the list of critical technologies on an annual or even semi-annual basis, deleting items from the list where appropriate and making all changes known to industry. The adoption of the Militarily Critical Technologies List is a first step in this direction. Inputs from industry are essential to identify technology already in the public domain or available in the world market from non-U.S. sources. Once we have simple guidelines and more current information on critical technologies, industry will be able to

assist government more effectively in protecting critical technologies.

If technology transfer control is important in protecting the national security, the Congress must provide the Government agencies involved in technology transfer issues with sufficient resources to consider industry requests promptly and efficiently. COMSAT has lived through several examples in recent years of complex applications to provide technical assistance which have required more than a year to be processed. Often some of the technical experts reviewing our applications in government agencies perform this function only as a "collateral duty", sometimes affording it a low priority. There have been times when there was confusion regarding which agency or agencies, and which staff members in those agencies, were working on our cases. Meetings often required months to arrange. It proved difficult to maintain the interest of our potential customers for an entire year while we sought Government clearance; the corollary of beginning work pending clearance involved a risk and was therefore equally unappealing. If the control of technology transfer is important, the government agencies involved should be organized and staffed to provide expeditious service.

Furthermore industry should have access to people within the Government in positions of sufficient authority to give us a quick, informal reaction to proposed technology transfers. Often industry could avoid becoming involved in contract negotiations if we knew that the subject matter were extremely sensitive. The current rules require us to negotiate a full contract with the foreign customer, provide it to the Government, and wait for approval. This is not always a sound way to proceed in international business.

Government regulations should be applied uniformly. Many articles published by Government officials acknowledge that there are gaps both in the Government regulatory scheme and in its enforcement. It is difficult to accept a regulatory scheme where you have doubts as to whether others in your industry are receiving equal treatment.

Let me close with two general remarks. There seems to be a growing controversy regarding prior or contemporaneous review by the U.S. Government of technical papers to be presented at open conferences or published in technical journals. COMSAT people belong to many professional societies. Each year, our scientists and engineers generate hundreds of technical articles and present dozens of technical papers at open conferences. In U.S. industry

and academia in general, there are many thousands of papers on high-technology subjects which are presented or published every year. I take no issue with the premise that some of the topics are sensitive and detailed technical papers on these subjects may require prior coordination with the Government; papers dealing with encryption are a good example. But, as I am sure my colleagues from the universities will indicate, these issues have implications which extend far beyond the performance of contracts with foreign clients or the delivery of hardware overseas. The Government will never have the resources to review all these papers, nor should it. Thus, in this area, the Government must find ways to narrow the list of technologies, and it must provide the resources necessary to give a prompt answer to inquiries. At the present time it is very hard to find people in government willing to review these papers on more than an infrequent basis.

Finally, I should state that COMSAT has an internationally recognized research facility, COMSAT Laboratories, and I would be remiss in failing to mention that the more limits the Government places on the free transfer of technical information and on the interaction of scientists from around the world, the slower will be the developement of technology in the United States. It would be unreasonable to assume that the United States is ahead in

everything and that we have nothing to learn from our foreign colleagues.

In summary, while it is important to recognize the necessity for constraints on technology transfer to enhance our national security, it is also important to preserve the ability of our high technology industry to compete successfully in the international marketplace. This also has important national security implications. The task before us is to strike a balance between these very important interests.

I might indicate that the private sector has begun careful examination of some of these issues. The National Academy of Sciences, in conjunction with the National Academy of Engineering, has formed a new committee to study issues of technology transfer restrictions as they apply particularly to universities and technical societies. The study would be undertaken by a panel of national leaders, and would be supervised by the National Academy of Sciences Committee for Science, Engineering and Public Policy, chaired by George Low, the former NASA administrator. I have the honor of serving on that Committee and I believe it will produce a balanced and useful report.

Best Available Copy

Mr. GORE. Thank you very much, and thanks to all of you.

Mr. Walgren.

Mr. WALGREN. Thank you, Mr. Chairman.

I wish I had been able to be here throughout the morning to hear the presentations.

Dr. Gerjuoy, I am interested in your reference to the impact on engineers that might occur if we were to have a system of voluntary publication censorship. It is more implied, I think, than developed in your statement.

Do you feel that a voluntary censorship system would really impede us across the board, particularly in the engineering area where we have so much to do in this country?

Dr. GERJUOY. Well, in general, I take it as a given, that if you impede communication between engineering research scientists, just as between physical scientists, you have to expect that you're going to cause duplication, that you're going to cause people to take false starts, and you're also going to lose certain kinds of satisfactions which Congressman Brown referred to very eloquently, I thought, in the testimony inserted in the Congressional Record on February 25 of this year.

People do get a great deal of satisfaction out of being able to talk to their colleagues, to have their work appreciated, to see their work published, to feel that they have beaten out the whole world in a problem and know that the whole world knows about it. This is all part of it.

Now, a great part of our university training is working with graduate students, and you don't develop these graduate students in this country unless they have some real desire and hope that a certain kind of life will accrue to them if they do go on to science and engineering.

I think it is clear that the kinds of restrictions that are being talked about in this society are of the kind that normally would tend to detract rather than attract young students to the sciences and to engineering. All this together I think has to have a deleterious effect.

Now, one cannot do it quantitatively. As I said in my testimony, it is not a quantitative affair. One has to have a gut feeling. But I think I really am representing the gut feeling of the engineering and scientific community in very large measure, and I urge, therefore, that somebody listen. I mean, there is a certain kind of merit in respecting this kind of feeling in a community which is patriotic like everybody else.

Mr. WALGREN. And then let me ask a question to the panel as a whole.

There was discussion this morning about the need for the various scientific and technical societies to make the first suggestions or to join in an evaluation of what might be done in this area of censorship and restraint.

Have any of your organizations been asked to review any of the administration's suggestions for restraint in this area, or has there been nothing coming from the administration thus far?

Dr. GERJUOY. In my role as chairman of the panel on public affairs last year, and in continuing to follow this subject, I have actu-

ally engaged in a dialog with various administration people and DOD and NSF and so on, trying to get this sort of review started.

Now, I think it is going forward. I do want to say that I am encouraged—for instance, in setting up the forum, which we heard about this morning, I think that is a very positive approach. The Department of Commerce has had conversations with John Crowley, who is executive director of the Association of American Universities, to set up a similar dialog with Commerce. I don't know of anything specifically with State as yet.

I am disappointed that the forum has not had a wider representation and is concentrated all in the university community, but there has not been a specific approach asking us to review any of the administration's suggestions for restraint. The point I am trying to make is that there is a tendency for these suggestions to get set in concrete, and it may be of interest that one of the President's men who reviews regulations—I ought to have his name; I have a note here—has said that he thinks it would be a very good idea if the administration did adopt an approach of having regulations of this kind reviewed before they are promulgated. I can give you a cite to that speech which was made in October.[1]

Mr. GORE. Thank you.

Others on the panel?

Dr. CORELL. Not to my knowledge has there been an approach to the land grant or sea grant university associations. I know it is true of the sea grant community. I will doublecheck for you with Robert Clodius, the president of the land grant. But to the best of my knowledge—and we have had some discussions—the issue was not referred to them. Therefore, to the best of my knowledge, there has been no contact with those two associations.

Dr. MCLUCAS. I don't know of any contacts, Mr. Walgren.

Mr. WALGREN. Thank you, Mr. Chairman.

Mr. GORE. Mr. Brown.

Mr. BROWN. Mr. Chairman, you referred earlier to the fact that the Chamber of Commerce had chosen not to appear at these hearings. But I have two letters, one dated earlier this month, and one in a similar situation a year ago, outlining their basic position with regard to restrictions on technological trade. I would like to ask unanimous consent that these two letters from the president of the U.S. Chamber of Commerce be included in the record as an indication of their position on this issue.

Mr. GORE. Without objection, we will put them in the record.

(See appendix, Letters From Chamber of Commerce of the United States of America to the U.S. Trade Representative, p. 264-269.)

Mr. BROWN. Dr. McLucas, I have been concerned about some specific cases of where we may have overly classified technical information to the detriment of our private industrial or economic development. I would like to specifically raise an issue which is going to be debated fairly extensively in the near future, having to do with the classification of Earth resources satellite observing technologies, which I think you are fairly familiar with.

---

[1] C. Boyden Gray, counsel to the Presidential Task Force on Regulatory Relief, in an address October 21, 1981, reported in the Environment Reporter, Current Developments, October 30, 1981, p. 819.

As you know, we have a large amount of classified technology in this area, and then we have the unclassified Landsat technology. We're in a situation where we perhaps might be on the verge of large-scale commercial applications and where we face a developing international competition from our friends, not our enemies, in this case.

I wonder if you would comment, without being exhaustive, as to whether or not the existence of a large body of classified technology and data here, may have had an effect on the development both of technology and policy with regard to unclassified civilian application in this field, both domestically and overseas?

Dr. McLucas. Well, Mr. Brown, I think that the existence of a large body of classified technology has had an effect in, shall I say, teaching industry how to extrapolate the technology into new areas. It seems to me that the support which the Government has given to certain technologies of that type could not have been other than helpful to the industry as a whole, and there is bound to be some spinoff from that in spite of the very strict security restrictions that apply.

I think that the fact that it is known that high resolution photography has military significance has worked to the detriment of proper exploitation of Landsat type of material. It seems to me that again we have to look for that balance, and in my view, the balance can only be struck by people who have a broad knowledge of the civilian needs and also the military capabilities and the military threats that the country faces. But I believe that more should have and could have been done to make the Landsat system more productive and that the results of those more productive systems could have been very helpful in a number of ways to the economy at large.

Mr. Brown. I have a feeling—and I'm speaking in ignorance of the classified information, of course—that the considerations which may have led to this classification were in the area which Admiral Inman described as relating to the "national interest" rather than the "national security," and yet I have no way of determining that, absent access to the full background on this development. That is one of the factors that leads me to raise the question of how important decisions were to be made in this area.

This committee, of course, has a long standing and a very intense interest in the commercialization of civilian space technology, and the question that arose in another subcommittee is whether this commercialization of civilian space technology was being impeded or not impeded, as the case may be, by the existence of this body of classified technology.

Dr. McLucas. If I may say another word on that, as I said earlier, I think the guidelines on what constitutes technology which should be closely held should be frequently updated. As the general technical community advances in making higher levels of technology practical, those guidelines should shift and recognize that what was once considered high resolution photography is now just ordinary material.

Mr. Brown. Let me ask you another question that again borders on the national interest versus the national security area.

97-341 O - 82 - 11

In the field of communications, this country has long been a strong supporter of what we call the free flow of information, and has run afoul of the less developed nations—the group of 77 specifically—on this concept of the New World Information Order, that they should be able to control the flow of information, essentially.

I raise the question with you as to the posture that this country is placed in if we decide that they were right after all, and that we should emulate them by controlling the free flow of information in the sense that we are seeking to put restrictions on this hemorrhaging of scientific and technical information that might be adversely used. Of course, that is exactly the argument that they use in wanting to curtail the flow of information from their countries, that it would be deleterious to their domestic well being.

Can you say something about that apparent contradiction?

Dr. McLucas. Well, Mr. Brown, I view with the same alarm as you any proposed change in our posture in that respect. I am very proud of the posture that we have taken to date, and I certainly hope that it can continue and that people like you and others on this committee would use their influence to keep us on the straight and narrow here.

Mr. Brown. We hope our influence can have that effect, Mr. McLucas.

I have no further questions, Mr. Chairman.

Mr. Gore. Well stated.

I would like to thank our witnesses—Dr. Corell, Congressman Judd Gregg has made the committee well aware of your expertise and he wanted to say those kind words publicly. He has an obligation at another committee. He was earlier here, of course, and wanted to be back for this panel but could not.

I would like to thank all of you for joining us and, indeed, the other witnesses who have been with us throughout the day as well. We will continue our interest in this subject and thanks to all the witnesses.

The hearing is adjourned.

[Whereupon, at 1:06 p.m., the subcommittees adjourned.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Soviet Acquisition of Western Technology

April 1982

Contents

	Page
Introduction	1
Soviet Acquisition of Western Technology: A National-Level Program	1
Soviet Mechanisms for Acquiring Western Technology	2
Soviet Acquisitions and Benefits	5
Outlook for the 1980s	11
Appendix	
Projected Soviet Technological Needs and Acquisition Targets Through the 1980s	13

Soviet Acquisition of Western Technology

Introduction

The United States and its Allies traditionally have relied on the technological superiority of their weapons to preserve a credible counterforce to the quantitative superiority of the Warsaw Pact. But that technical superiority is eroding as the Soviet Union and its Allies introduce more and more sophisticated weaponry—weapons that all too often are manufactured with the direct help of Western technology.[1] Stopping the Soviets' extensive acquisition of military-related Western technology—in ways that are both effective and appropriate in our open society—is one of the most complex and urgent issues facing the Free World today.

This report describes the Soviet program to acquire US and Western technology, the acquisition mechanisms used, the spectrum of Western acquisitions that have contributed to Soviet military might, the projected Soviet priority needs for Western technology, and the problems of effectively stemming the transfer of Western technology that could someday find application in weapons used to threaten the West.

Soviet Acquisition of Western Technology: A National-Level Program

Since at least the 1930s, the Soviet Union has devoted vast amounts of its financial and manpower resources to the acquisition of Western technology that would enhance its military power and improve the efficiency of its military manufacturing technology. Today this Soviet effort is massive, well planned, and well managed—a national-level program approved at the highest party and governmental levels.

[1] While there are numerous interpretations of "technology" for weapons, it is defined in this report as the application of scientific knowledge, technical information, know-how, critical materials, keystone manufacturing and test equipment, and end products which are essential to the research and development as well as the series manufacture of modern high-quality weapons and military equipment. Western technology is defined as that technology developed by the Free World.

This program accords top priority to the military and military-related industry, and major attention is also given to the civilian sectors of Soviet industry that support military production.

The Soviets and their Warsaw Pact allies have obtained vast amounts of militarily significant Western technology and equipment through legal and illegal means. They have succeeded in acquiring the most advanced Western technology by using, in part, their scientific and technological agreements with the West to facilitate access to the new technologies that are emerging from the Free World's applied scientific research efforts; by spending their scarce hard currency to illegally purchase controlled equipment, as well as to legally purchase uncontrolled advanced Western technologies having military-industrial applications; and by tasking their intelligence services to acquire illegally those US and Western technologies that are classified and export controlled.

The Soviets have been very successful in acquiring Western technology by blending acquisitions legally and illegally acquired by different government organizations. The Soviet intelligence services—the Soviet Committee for State Security (KGB) and the Chief Intelligence Directorate of the Soviet General Staff (GRU)—have the primary responsibility for collecting Western classified, export-controlled, and proprietary technology, using both clandestine and overt collection methods. They in turn make extensive use of many of the East European Intelligence Services (see inset, p. 2); for their efforts in acquiring Western technology, these countries are paid in part with Soviet military equipment and weapons.

Clandestine acquisition of the West's most advanced military-related equipment and know-how by the KGB and GRU is a major and growing problem.

Best Available Copy

East European Intelligence Services Acquire Technologies for the Soviet Union

In the late 1970s a former East European intelligence officer revealed organizational and targeting details related to Soviet-directed acquisitions of Western technology by East European intelligence services, particularly military-industrial manufacturing-related technologies that were given the highest priority for collection by at least one East European intelligence service. Many technologies were acquired through dummy firms established in Western Europe that were successful in securing some of the most advanced technologies in the West, including computer, microelectronic, nuclear, and chemical technologies.

In microelectronics, for example, many US firms were targeted through their affiliates in Western Europe; scientists, technicians, and commercial representatives also were successfully recruited to provide information during their trips to Europe. Although most of the military and defense-industrial information acquired by East European intelligence services went to the Soviets, much of it was used by the East Europeans themselves to benefit their military and civilian industries. The computer, microelectronic, and photographic areas were priority targets. The East European countries benefited considerably from microelectronic acquisitions, and could not have achieved the present level of development in their computer industry without illegal acquisitions of Western technology.

These intelligence organizations have been so successful at acquiring Western technology that the manpower levels they allocate to this effort have increased significantly since the 1970s to the point where there are now several thousand technology collection officers at work. These personnel, under various covers ranging from diplomats to journalists to trade officials, are assigned throughout the world.

Soviet foreign trade organizations, or enterprises, although quasi-independent entities, are partially subordinated to the Ministry of Foreign Trade, and their activities are closely coordinated by this Ministry. They have major responsibilities for both legal and illegal acquisitions and purchases; they work closely with the KGB and GRU in arranging trade diversions. East European trade companies assist them in clandestine and illegal acquisition operations.

Official Soviet and East European science and technology (S&T) organizations also play a major role in both open and clandestine acquisition of Western technology. The Soviet State Committee for Science and Technology (GKNT) is the key player in arranging government-to-government science and technology agreements to facilitate access to and the acquisition of established as well as new technologies, including those just emerging from Western universities, laboratories, and high-technology firms. It is the GKNT that oversees the allocation of scarce Soviet hard currency for the legal purchase by various Soviet organizations of selected Western technology for Soviet military purposes. If the GKNT is unable to acquire the necessary technology by open or legal means, it tasks Soviet intelligence to clandestinely acquire the technology.

It is the well-organized and well-coordinated use of all these organizations that has made the Soviet program to acquire Western technology so successful. As a result, the Soviets have acquired militarily significant technologies and critically important industrial Western technologies that have benefited every major Soviet industry engaged in the research, development, and production of weapon systems.

Soviet Mechanisms for Acquiring Western Technology

Soviet acquisition mechanisms include: *legal means* through open literature, through legal trade channels, and through student scientific and technological exchanges and conferences; *illegal means* through trade channels that evade US and Western (i.e. CoCom)[1] export controls, including acquisitions by their intelligence services through recruited agents and industrial

[1] The Coordinating Committee (CoCom) was established in 1949 to serve as the forum for Western efforts to develop a system of strategic export controls. It is composed of the United States, the United Kingdom, Turkey, Portugal, Norway, the Netherlands, Luxembourg, Japan, Italy, Greece, France, the Federal Republic of Germany, Denmark, Canada, and Belgium.

Best Available Copy

espionage. While a large volume of technology is acquired by nonintelligence personnel, the overwhelming majority of what the United States considers to be militarily significant technology acquired by and for the Soviets was obtained by the Soviet intelligence services and their surrogates among the East European intelligence services. However, legal acquisitions by other Soviet organizations are important since it is often the combination of legally and illegally acquired technologies that gives the Soviets the complete military or industrial capability they need.

Because of the priority accorded to the military over the civilian sectors of the Soviet economy, Western dual-use technology—i.e., technology with both military and civilian applications—almost always finds its way first into military industries, and subsequently into the civilian sectors of industries that support military production. Thus, Soviet assurances that legally purchased dual-use technology will be used solely for civilian applications can seldom be accepted at face value.

Legal acquisitions generally have their greatest impact on the Soviets' broad industrial base, and thus affect military technology on a relatively long-term basis. The Soviet Kama Truck Plant, for example, was built over some seven years with massive imports of more than $1.5 billion worth of US and West European automotive production equipment and technology. Large numbers of military-specification trucks produced there in 1981 are now being used by Soviet forces in Afghanistan and by Soviet military units in Eastern Europe opposite NATO forces. Similarly, large Soviet purchases of printed circuit board technology and numerically controlled machine tools from the West already have benefited military manufacturing sectors.

The Soviets give priority to those purchases that meet the direct needs of the Soviet military-industrial complex by paying for them in hard currency. Over the past 10 years, the Soviets legally and illegally purchased large quantities of Western high-technology microelectronics equipment that has enabled them to build their own military microelectronics industry in a short time. This acquired capability in microelectronics is the critical basis for the present wide-ranging enhancements of Soviet military systems and for their continuing sophistication.

Acquisitions through illegal trade channels often have both industrial and military applications, and thus are important in the near term. Illegal acquisitions of technology fall into two general categories, both of which are extremely difficult to detect and monitor. One is the diversion of controlled technology from legitimate trade channels to proscribed destinations. This is done through US and foreign firms that are willing to engage in profitable impropriety; through agents-in-place in US or foreign firms or foreign subsidiaries of US firms; through Soviet- and East European—owned firms locally chartered in the West; and through foreign purchasing agents (including arms dealers). For instance, to evade the US embargo on microelectronic technology exports to the Soviet Union, the Soviets and their surrogates have set up dummy corporations in the West that purchase sophisticated microelectronics manufacturing equipment. This equipment is then shipped and reshipped, sometimes with the knowledge of individuals in the companies, to disguise its ultimate destination—the Soviet Union or Eastern Europe. Both the Soviet and Warsaw Pact intelligence services are in the mainstream of this illegal technology trade flow. The other type of diversion is an in-place diversion, in which legally acquired technology and equipment—in the computer area, for example—are put to military end uses not authorized in export license applications.

The acquisitions that most directly affect Soviet military development have come from intelligence collection and related illegal trade diversions. Soviet Bloc intelligence services have concentrated their effort in the United States, Western Europe, and Japan. These services target defense contractors and high-technology firms working on advanced technology (both classified and unclassified), foreign firms and subsidiaries of US firms abroad, and international organizations with access to advanced and/or proprietary technology, including access to computer data base networks throughout the world.

Best Available Copy

Table 1

Major Fields of Technology of Interest to Soviet and East European Visitors to the United States

Computers	Architecture Automatic Control CAD (Computer-Aided Design) Cybernetics/Artificial Intelligence Data Bases Image Processing Design Image Processing/Retrieval	Memories N/C (Numerically Controlled) Units Networks Pattern Recognition Programming Robots Software
Materials	Amorphous CAD Composites Cryogenics Deformation	Metallurgy N/C Machine Tools Powder Metals Superconductors Testing/NDT (Non-Destructive)
Semiconductors	CAD Circuits Defects Devices	Design Ion Implantation Production Technology SAW (Surface Acoustic Wave) Devices
Communications, Navigation, and Control	Antennas Microwave/Millimeter Waves Radio Wave Propagation	Satellite Communications Signal Processing Telecommunications
Vehicular/Transportation	Marine Systems	Shipbuilding
Laser and Optics	Fiber Optics Gas Lasers	Optics Tunable Lasers
Nuclear Physics	Cryogenics Fusion Materials MHD (Magnetohydrodynamics)	Reactors Structural Designs Superconductors
Microbiology	Genetic Engineering	

Both legal and illegal acquisitions of US and Western technology and equipment are coordinated with information obtained through the complex network of international governmental scientific and technical agreements and exchanges that the USSR maintains with the advanced industrial nations. These include know-how, equipment, and computer data base collection activities of Soviet scientists and engineers who participate in academic, commercial, and official S&T exchanges. Visiting Soviet and East European technical and student delegations to the United States generally consist of expert scientists, many of whom are connected with classified work in their home countries. Such was the case with the Soviet scientist who managed to get assigned to fuel-air explosives work. When he finished his US study programs, he almost certainly returned to the USSR to work on related weapons. Other Soviet and East European scientists have come to the United States to work in the aerohydrodynamic, cryogenic, optic, laser, computer, magnetic bubble computer memory, nuclear, microelectronic, and structural and electronic material areas. Given the military importance of these fields to the Soviet Union, it appears likely that a high percentage of these scientists will work on military-related programs in these areas after they return home.

From the beginning, Soviet candidates in various academic and scientific exchange programs have nearly always proposed research activities involving technologies in areas that have direct military applications and in which the Soviets are technologically deficient. Table 1 provides a list of the key high-technology fields that Soviet and East European

Best Available Copy

visitors come to the United States to study, research, or discuss, many of which are on the US Militarily Critical Technology List today. In each of the past two years, more than a third of the 50 program proposals offered under the Graduate Student/Young Faculty Program of the International Research and Exchanges Board (IREX) has been completely unacceptable in terms of prospective technology loss, and many other programs needed to be modified or have access constrained before the exchanges could be allowed.

The Soviets correctly view the United States and several other Western countries as a continuing source of important and openly available scientific and technical information, which they take every opportunity to obtain access to. Some of the unclassified documents so acquired are previously classified materials which had been downgraded to unclassified through US procedures providing for automatic declassification after a stipulated period. When collected on a massive scale and centrally processed by the Soviets, this information becomes significant because it is collectively used by Soviet weapons designers and weapons countermeasure experts.

The Soviets also regularly attend high-technology trade shows, and attempt to visit commercial firms in the West, particularly small and medium-sized firms that are active in developing new technologies. These apparent trade promotion efforts often mask Soviet attempts to acquire emerging Western technological know-how before its military uses have been identified and government security controls have been applied. Emerging technologies are particularly vulnerable to foreign collection efforts of this type.

Soviet intelligence continues to place a high priority on the collection of S&T information on genetic engineering and futuristic weapons such as lasers and particle beam weapons. The Soviets have been stepping up their efforts to acquire new and emerging technologies such as very-high-speed integrated-circuit (VHSIC) and very-large-scale integration (VLSI) technology from Western universities and commercial laboratories for both military and commercial applications.

Over the past few years there has been an increased use of Soviet- and East European–owned firms locally chartered in the United States and abroad to exploit Western-controlled and military-related technology. There are more than twenty Soviet- and East European–owned firms in the United States, and near the end of the 1970s there were more than 300 similar firms in Western Europe. In addition to the United States, heavy concentrations are in the United Kingdom, Sweden, the Netherlands, Italy, the Federal Republic of Germany, France, Canada, Belgium, and Austria. These firms are avenues for Soviet acquisition of advanced Western technologies, as was shown when the US engineer arrested in late 1981 was charged with selling US secret documents to an East European intelligence officer employed by a Polish-owned firm chartered in Illinois (see inset, p. 6). Furthermore, firms chartered in the United States can legally purchase controlled US technology and study it without actually violating US export controls unless they attempt to export the equipment or related technical data from the United States without a license.

Soviet Acquisitions and Benefits

Today's recognition of the crucial role of Western technology in the development and production of Soviet weapon systems and related military equipment is not unique. Soviet dependence on Western technology was visible and clear-cut in the years immediately after World War II, when the Soviets stole Western nuclear secrets leading to their development of a nuclear weapon capability, and copied a US bomber in its entirety leading to production of their TU-4. To achieve major improvements in their military capability quickly, they exploited captured scientists and industrial plants and resorted to a combination of espionage, stealing, and copying Western systems.

Since that early period of near-complete reliance in the 1950s, the Soviets' dependence on Western technology to develop their weapons has decreased. Nevertheless, despite several decades of Soviet priorities focused on science, technology, and weapon systems, the Soviets, because of their inability to be innovative

Best Available Copy

US Radar Expert Passes Over 20 Significant Classified Reports on Future US Weapon Systems to Intelligence Agent

William H. Bell, a radar project engineer for a high-technology US defense firm was recruited by an intelligence officer who operated under cover as a vice president of the Polish firm called Polamco. This firm is a subsidiary of the Polish Government Corporation and is incorporated in Illinois and Delaware. It began as an importer/exporter of machinery, parts and tools and as a consultant to firms exporting these products to Poland. The recruitment began as a simple friendship between neighbors with mutual sporting interests, grew quickly to include their families, then to proving Bell's credentials by showing a classified document to the agent, and then to passing microfilm copies of classified reports at meeting places in the US, Switzerland, and Austria. Mr. Bell was in financial straits and was easily influenced by the cash proffered—a total of $110,000 over a three-year period. In all, over 20 highly classified reports on advanced future US weapon systems or their components were passed to the Polish Intelligence Service and probably eventually to the Soviet Intelligence Service.

Among the classified reports, those of prime importance to the West included: the F-15 look-down-shoot-down radar system, the quiet radar system for the B1 and Stealth bombers, an all-weather radar system for tanks, an experimental radar system for the US Navy, the Phoenix air-to-air missile, a ship-borne surveillance radar, the Patriot surface-to-air missile, a towed-array submarine sonar system, a new air-to-air missile, the improved HAWK surface-to-air missile, and a NATO air-defense system. The information in these documents put in jeopardy existing weapons and advanced future weapon systems of the United States and its Allies. The acquisition of this information will save the Polish and Soviet Governments hundreds of millions of dollars in R&D efforts by permitting them to implement proven designs developed by the United States and by fielding operational counterpart systems in a much shorter time period. Specifications on current and future US weapon systems will enable them to develop defensive countermeasure systems.

and effectively apply new technology to weapons developments, still depend on Western technology and equipment to develop and manufacture some of their advanced weapon systems more quickly.

Today, Soviet military designers carefully choose the Western designs, engineering approaches, and equipment most appropriate to their deficiencies and needs. These needs are still substantial and pervade almost every area of weapons technology and related manufacturing equipment. Table 2 lists classes of Western technology acquired by the Soviets and East Europeans and illustrates the wide range of Soviet military technology needs. In the following paragraphs of this section, Soviet Bloc acquisitions have been grouped according to their likely applications: strategic systems, aircraft systems, naval systems, and tactical systems. Also cited are acquisitions in the microelectronic and computer areas that have broad application to military and industrial programs. In certain of these areas, notably the development of microelectronics, the Soviets would have been incapable of achieving their present technical level without the acquisition of Western technology. In other areas, acquisitions have allowed the Soviets to reduce the indigenous effort they would otherwise have had to expend.

The Soviets' strategic weapons program has benefited substantially from the acquisition of Western technology. The striking similarities between the US Minuteman silo and the Soviet SS-13 silo very likely resulted from acquisition of US documents and expedited deployment of this, the first Soviet solid-propellant ICBM. The Soviets' ballistic missile systems in particular have, over the past decade, demonstrated qualitative improvements that probably would not have been achieved without Western acquisitions of ballistic missile guidance and control technology. The most striking example of this is the marked improvement in accuracy of the latest generation of Soviet ICBMs—an improvement which, given the level of relevant Soviet technologies a decade ago, appears almost certainly to have been speeded by the acquisition of Western technology. Their improved accuracy has been achieved through the exploitation and development of good-quality guidance components—such

Best Available Copy

Table 2

Selected Soviet and East European Legal and Illegal Acquisitions From the West Affecting Key Areas of Soviet Military Technology

Key Technology Area	Notable Successes
Computers	Purchases and acquisitions of complete systems designs, concepts, hardware and software, including a wide variety of Western general purpose computers and minicomputers, for military applications.
Microelectronics	Complete industrial processes and semiconductor manufacturing equipment capable of meeting all Soviet military requirements, if acquisitions were combined.
Signal Processing	Acquisitions of processing equipment and know-how.
Manufacturing	Acquisitions of automated and precision manufacturing equipment for electronics, materials, and optical and future laser weapons technology; acquisition of information on manufacturing technology related to weapons, ammunition, and aircraft parts including turbine blades, computers, and electronic components; acquisition of machine tools for cutting large gears for ship propulsion systems.
Communications	Acquisitions of low-power, low-noise, high-sensitivity receivers.
Lasers	Acquisitions of optical, pulsed power source, and other laser-related components, including special optical mirrors and mirror technology suitable for future laser weapons.
Guidance and Navigation	Acquisitions of marine and other navigation receivers, advanced inertial-guidance components, including miniature and laser gyros; acquisitions of missile guidance subsystems; acquisitions of precision machinery for ball bearing production for missile and other applications; acquisition of missile test range instrumentation systems and documentation and precision cinetheodolites for collecting data critical to postflight ballistic missile analysis.
Structural Materials	Purchases and acquisitions of Western titanium alloys, welding equipment, and furnaces for producing titanium plate of large size applicable to submarine construction.
Propulsion	Missile technology; some ground propulsion technology (diesels, turbines, and rotaries); purchases and acquisitions of advanced jet engine fabrication technology and jet engine design information.
Acoustical Sensors	Acquisitions of underwater navigation and direction-finding equipment.
Electro-optical Sensors	Acquisition of information on satellite technology, laser rangefinders, and underwater low-light-level television cameras and systems for remote operation.
Radars	Acquisitions and exploitations of air defense radars and antenna designs for missile systems.

as gyroscopes and accelerometers. The quality of these instruments, in turn, depends to a considerable degree on the quality of the small, precision, high-speed bearings used.

Through the 1950s and into the 1960s, the Soviet precision bearing industry lagged significantly behind that of the West. However, through legal trade purchases in the 1970s, the Soviet Union acquired US precision grinding machines for the production of small, high-precision bearings. Similar grinding machines, having lower production-rate capabilities, were available from several foreign countries. Only a few of these machines, either US or foreign, would have been sufficient to supply Soviet missile designers with all the quality bearings they needed. These purchases provided the Soviets with the capability to manufacture precision bearings in large volume sooner than would have been likely through indigenous development. The Soviets probably could have used indigenous grinding machines and produced the required quality of bearings over a long period by having an abnormally high rejection rate.

While some of the Soviet acquisition in the aircraft area appears directed toward the development of countermeasures against Western systems, the Soviets appear to target data on Western aircraft primarily to acquire the technology. Furthermore, while the Soviets have acquired a large amount of hardware and data from planes downed or captured in Vietnam and elsewhere, they continue to attempt to acquire the most advanced technologies through both legal and illegal transactions with the West. Assimilation of

Best Available Copy

Western technology has been of great benefit to both their military and commercial aircraft development programs—to the extent that aircraft from certain Soviet military design bureaus are to a significant degree copies of aircraft of Western design. Soviet military aircraft designers have "ordered" documents on Western aircraft and gotten them within a few months, including plans and drawings for the US C-5A giant transport aircraft early in its development cycle; these plans, although dated now, have contributed to current Soviet development of a new strategic military cargo plane. Designers were in particular need of data on US technological advances, but more importantly, they needed information on aerospace manufacturing techniques.

Soviet aircraft designers have been interested in US military transports and wide-body jets and probably have managed to accelerate the development programs for their IL-76 Candid and IL-86 transports. The IL-86 looks much like the Boeing 747 and the IL-76 resembles the C-141. Neither system is an identical copy.

The IL-76 also is used by the Soviets as the platform for their new AWACS (Airborne Warning And Control System), which is expected to be operational in the mid-1980s. This system will provide the Soviets with a major improvement in attacking low-flying missiles and bombers. The Soviet AWACS is strikingly similar in many ways to the US AWACS, and is a major improvement over their old AWACS.

The Soviets' acquisition effort in the naval systems area reflects well the two major factors that motivate their requirements: the acquisition of technology not readily available to them—yet critical to their programs—and the acquisition of equipment which, while producible in the Soviet Union, allows them to divert resources to more pressing naval programs. The Soviets appear to have concentrated their acquisitions in areas related to aircraft carriers, deep sea diving capabilities, sensor systems for antisubmarine warfare and navigation, and ship maintenance facilities. In the maintenance area, two huge floating drydocks purchased from the West for civilian use by the Soviets have been diverted to military use. Drydocks are critical for both routine and fast repair of ships damaged in warfare. In 1978, when the Soviets took possession of one of the drydocks, they diverted it to the Pacific Naval Fleet. The other was sent to the Northern Fleet in 1981.

These drydocks are so large that they can carry several naval ships. More importantly, they are the only drydock facilities in either of the two major Soviet fleet areas—Northern or Pacific—capable of servicing the new Kiev-class V/STOL aircraft carriers. Soviet advanced submarines carrying ballistic missiles, Soviet Kiev aircraft carriers, and Soviet destroyers were among the first ships repaired in these drydocks. It is important to note that the drydocks themselves are so large that no Soviet shipyard would have been capable of accommodating their construction without major facility modifications, associated capital expenditures, and interruptions in present weapons programs. Their importance will be even more pronounced when the Soviets construct the still-larger carriers (for high-performance aircraft) projected for the 1990s. The Soviets even have acquired Western aircraft carrier catapult equipment and documentation for this larger carrier; catapult technology, though relatively common in the West, is outside the Soviet experience.

Within the past few years, the USSR also has contracted for or purchased foreign-built oceanographic survey ships equipped with some of the most modern Western-manufactured equipment. In place of US equipment that was embargoed, other Western equipment has been installed on the ships. This modernization of what is the world's largest oceanographic fleet with Western technology will help support the development of Soviet weapon system programs and antisubmarine systems against the West.

Although the Soviets have a strong indigenous technology base that could support the development of much of their tactical weapons systems, this does not prevent them from maintaining an ambitious program for acquiring and benefiting from Western technology in this area. In some cases, their acquisitions satisfy deficiencies in Soviet technology; smart weapons technology and electro-optical technology are examples of

Best Available Copy

Table 3

Microelectronic Equipment and Technology Legally and Illegally Acquired by the Soviet Bloc

Equipment or Technology	Comments
Process Technology for Microelectronic Wafer Preparation	The Soviets have acquired hundreds of specific pieces of equipment related to wafer preparation, including expitaxial growth furnaces, crystal pullers, rinsers/dryers, slicers, and lapping and polishing units.
Process Technology for Producing Circuit Masks	Many acquisitions in this area include computer-aided design software, pattern generators and compilers, digital plotters, photorepeaters, contact printers, mask comparators, electron-beam generators, and ion milling equipment.
Equipment for Device Fabrication	Many hundreds of acquisitions in this area have provided the Soviets with mask aligners, diffusion furnaces, ion implanters, coaters, etchers, and photochemical process lines.
Assembly and Test Equipment	Hundreds of items of Western equipment, including scribers, bonders, probe testers, and final test equipment have been acquired by the Soviets.

this. Signal and information-processing technology, particularly for Soviet air defense systems, is another. More often, however, technology is exploited to speed up a developmental program or to improve upon original Western designs in an expeditious manner. The Soviets appear to have concentrated their tactical systems acquisitions on Western tank, antitank, and air defense–related technology and equipment in order to derive concepts and know-how to benefit their weapons programs and to design countermeasures to the Western systems. The Soviet SA-7 heat-seeking, shoulder-fired antiaircraft missile contains many features of the US Redeye missile. Such acquisitions have enabled the Soviets to obtain advanced tactical weapon capabilities sooner than otherwise would have been possible.

Western equipment and technology have played a very important, if not crucial, role in the advancement of Soviet microelectronic production capabilities. This advancement comes as a result of over 10 years of successful acquisitions—through illegal, including clandestine, means—of hundreds of pieces of Western microelectronic equipment worth hundreds of millions of dollars to equip their military-related manufacturing facilities. These acquisitions have permitted the Soviets to systematically build a modern microelectronics industry which will be the critical basis for enhancing the sophistication of future Soviet military systems for decades. The acquired equipment and know-how, if combined, could meet 100 percent of the Soviets' high-quality microelectronic needs for military purposes, or 50 percent of all their microelectronic needs.

Table 3 identifies the microelectronic production-related equipment that has been acquired by the Soviet Bloc. These acquisitions have been grouped into areas related to the four steps required to produce a microchip: wafer preparation, circuit-mask making, device fabrication, and assembly and testing.

Soviet computer technology has long been limited by fabrication and production technology problems and by difficulties in software development. Since 1969 the USSR and East European countries have been developing a family of general purpose computers known as the Ryad series. These computers, which make up virtually the total Soviet and East European effort in large general purpose computers, have been and will continue to be used in a wide variety of civil and military applications. Western technology has been important to development of the Ryad series by providing proven design directions both at the system and component levels. The architectural designs of the

Best Available Copy

Ryad computers, for example, are patterned after those of the highly successful mass produced IBM 360 and 370 series, computers that are used in a wide range of applications and are highly serviceable in the field.

With this approach, the Soviets and East Europeans eliminated many of the risks involved in undertaking the development and production of a new series of general purpose computers, and saved considerable amounts of manpower and time. Since the early 1970s the Soviets and East Europeans have legally purchased more than 3,000 minicomputers, some of which are now being used in military-related organizations. Furthermore, they are also developing minicomputers that are direct copies of Western models. Soviet and East European development of computer systems has been aided by all available means—legal and illegal, including clandestine—for acquiring the needed technical know-how.

Thus, the Soviets and their Warsaw Pact allies have derived significant military gains from their acquisitions of Western technology, particularly in the strategic, aircraft, naval, tactical, microelectronics, and computer areas. This multifaceted Soviet acquisitions program has allowed the Soviets to:

- Save hundreds of millions of dollars in R&D costs, and years in R&D development lead time (see inset).
- Modernize critical sectors of their military industry and reduce engineering risks by following or copying proven Western designs, thereby limiting the rise in their military production costs.
- Achieve greater weapons performance than if they had to rely solely on their own technology.
- Incorporate countermeasures to Western weapons early in the development of their own weapon programs.

These gains are evident in all areas of military weapons systems. While difficult to quantify, it is clear that the Western military expenditures needed to overcome or defend against the military capabilities derived by the acquisition of Western technology far outweigh the West's earnings from the legal sales to the Soviets of its equipment and technology.

Soviet Intelligence Officer Reveals Technology Acquisition Saved Soviet Military Hundreds of Millions of Rubles

A former Soviet intelligence officer revealed that information on Western military-related technology acquired by the Soviet intelligence services saved the Soviet military industry hundreds of millions of rubles. The acquisition of Western technology operationally was assigned the highest priority for collection by local residencies in key West European countries because of the relatively easy access to much US and Western technology in Europe and the praise being received by the services for their acquisition efforts.

These acquisitions were directed by the military manufacturing industries under the Council of Ministers, and there was intense competition between the intelligence services to acquire Western technology needed for weapons development programs. Of particular need by Soviet weapons designers has been the acquisition of knowledge on special materials, notably the weaving of carbon filaments in a three dimensional configuration which the services were tasked to acquire. The end products from this 3-D carbon-carbon weaving technology are useful for ablative heat shields for high velocity reentry vehicles (the warhead part of ICBMs and SLBMs) and for other portions of rocket motors for large missiles. The Soviet acquisition of some of this technology is likely to enable them to eventually gain a capability for increased military options against the West—a capability that otherwise would have taken them several additional years to develop themselves. The intelligence services also worked closely with scientists from the Soviet military manufacturing industries and even planned joint operations against Western Trade and Equipment Fairs in order to acquire needed Western technology.

Best Available Copy

Outlook for the 1980s

The Soviets' military R&D and weapon test-and-evaluation efforts are continuing at a rapid pace. Several hundred development projects for weapons systems and major system elements are now under way, and it is expected that through the 1980s the number of new or modified advanced Soviet weapon systems emerging from these projects into production and deployment will remain at the high levels of the last two decades—some 200 weapon systems per decade.

Soviet military manufacturing capacity increased by a significant 80 percent during the 1960s and 1970s, and new plant expansion now under way at one-fourth of their key weapons manufacturing facilities will add considerably to their capabilities. These new facilities will be ready to produce weapons in the next four to 10 years. Plant expansion is in the following areas: ground warfare vehicles, including new tanks; aviation, including facilities for a new B-1-type bomber and a new long-range military transport aircraft having strategic airlift capabilities; naval shipbuilding, including submarines for ballistic missiles and cruise missiles, as well as full-size aircraft carriers for high-performance aircraft capable of competing with the United States in global operations; and electronic and microelectronic manufacturing facilities throughout the USSR. The development and production of new Soviet weapons at these facilities is sure to be more complex and costly than during the 1970s.

All of this military development and plant expansion activity, however, is taking place at a time when the Soviet economy has reached its lowest level of growth since World War II. Soviet annual GNP growth may well be limited to an average of 1 to 2 percent by the mid-1980s. Stagnation in industrial sectors that are key to both the civilian and the military sectors will make it increasingly difficult for the Soviets to satisfy the needs of both. Thus, Soviet leaders will have to make tough choices among defense, investment, and consumption; the competition among rival claimants for resources will become intense. Under these conditions, it may be impossible for the Soviets to maintain current growth in military production without hurting the civilian economy.

Despite these economic difficulties, there are no signs that the Soviets are shifting resources away from the military sector or slowing down development of weapon systems that will be entering the production stage by mid-decade. New generations of Warsaw Pact weapons will require selected critical component and modern manufacturing technologies. It is in these areas that Soviet illegal acquisitions of Western technology, complemented by legal acquisitions, are most likely to be concentrated over the next five to 10 years.

Among the more important technologies are microelectronics, computers, and signal processing. Microelectronics will play a very significant role in advances in computers and signal processing, and all of these technologies will be important in developing advanced Soviet missile, aircraft, naval, and tactical weapon systems, and associated detection systems. Additional projected Soviet technological needs related to such systems are presented in the appendix.

As the result of both tactical and strategic force modernizations, Soviet and Warsaw Pact military manufacturers are increasingly pressed by large-scale production requirements and the related need to control manufacturing and materials costs. Thus, particularly critical for the 1980s are Soviet needs to improve their manufacturing capability. To a large extent, the level of manufacturing technology in Soviet plants determines the Soviets' capability to move new technology from R&D into military applications. Manufacturing technologies play a significant role not only in the development of advanced component technologies, such as microelectronics and computers, but also in the actual production of modern military systems.

Future Soviet and Warsaw Pact acquisition efforts—including acquisitions by their intelligence services—are likely to concentrate on the sources of such component and manufacturing technologies, including:

- Defense contractors in the United States, Western Europe, and Japan who are the repositories of military development and manufacturing technologies.

Best Available Copy

- General producers of military-related auxiliary manufacturing equipment in the United States, Western Europe, and Japan.

- Small and medium-size firms and research centers that develop advanced component technology and designs, including advanced civil technologies with future military applications.

The combination of past Soviet acquisition practices and projected Soviet military needs indicates that the United States and its Allies are likely to experience serious counterintelligence and related industrial security and export control problems over the next five to 10 years.

The task of stopping Soviet Bloc intelligence operations aimed at Western military and industrial technologies already poses a formidable counterintelligence problem, both in the United States and abroad. But that task is likely to become even more difficult in the future as several trends identified in the 1970s continue into the 1980s:

- First, since the early 1970s, the Soviets and their surrogates among the East Europeans have been increasingly using their national intelligence services to acquire Western civilian technologies—for example, automobile, energy, chemicals, and even consumer electronics.

- Second, since the mid-1970s, Soviet and East European intelligence services have been emphasizing the collection of manufacturing-related technology, in addition to weapons technology.

- Third, since the late 1970s, there has been increased emphasis by these intelligence services on the acquisition of new Western technologies emerging from universities and research centers.

The combined effect of these trends is a heavy focus by Soviet Bloc intelligence on the commercial sectors in the West—sectors that are not normally protected from hostile intelligence services. In addition, the security provided by commercial firms is no match for the human penetration operations of such foreign intelligence services. But the most alarming aspect of this commercial focus by Soviet Bloc intelligence services is that as a result of these operations the Soviets have gained, and continue to gain, access to those advanced technologies that are likely to be used by the West in its own future weapons systems.

The Soviet intelligence effort against Western defense contractor firms poses a serious problem in itself. With more than 11,000 such firms in the United States and hundreds of subsidiaries abroad, US counterintelligence efforts are stretched thin. Protection of US firms abroad from hostile intelligence threats is the responsibility of host governments, but they too are feeling the burden of well-orchestrated Soviet Bloc efforts. The Soviet intelligence threat and the illegal trade problem appear to be severe in Japan. It appears that Western industrial security—both defense and commercial—will be severely tested by the Soviet intelligence services and their surrogates among the East European intelligence services during the 1980s.

Western industrial nations also can expect increased Soviet Bloc intelligence activities directed at the acquisition of their key industrial technologies. Western export controls are presently being updated and broadened; the CoCom allies have recently agreed to strengthen controls and to enhance their enforcement. Moreover, serious hard currency shortages, along with generally increased restrictions on Soviet S&T visitors to the United States, will make the Soviets even more dependent on intelligence and other illegal efforts to acquire the goods and equipment they will need.

The massive, well-planned, and well-coordinated Soviet program to acquire Western technology through combined legal and illegal means poses a serious and growing threat to the mutual security interests of the United States and its Allies. In response, the West will need to organize more effectively than it has in the past to protect its military, industrial, commercial, and scientific communities.

Best Available Copy

Appendix

Projected Soviet Technological Needs and Acquisition Targets Through the 1980s

Given the dynamic nature of their collection program, it is expected that the Soviets will continue their attempts to acquire a broad range of Western technologies. Certain areas, however, represent priority collection targets for them; these areas are critical to the Soviets' enhancement of their weapons capability.

Over the past decade, the Soviets' most pronounced improvements in strategic weaponry have been in the development of a MIRV ballistic missile capability and a significant improvement in the accuracy of their ICBMs. The former capability was made possible largely through the introduction of onboard digital computers and the latter through the improvement in the quality of the missile guidance systems and the procedures used to calibrate them. Technology acquisitions from the West contributed significantly to these improved capabilities.

The Soviets probably will continue to make their highest priority the acquisition of Western microelectronics and computer technology for in-flight guidance computers. This acquisition effort will be motivated by a desire to overcome reliability problems and also to provide the on-board processing capability required for the development of new guidance options with the potential for extremely high accuracies.

The Soviets will also give top priority to acquiring information on the latest generation of US-inertial components upon which the MX ICBM and the Trident SLBM guidance systems are based. Despite the past accuracy improvements of Soviet ICBMs, these two US systems incorporate technologies beyond present Soviet technological capabilities. Moreover, their SLBM accuracies are significantly behind those of US systems. In addition to information on hardware, the Soviets are expected to seek calibration software algorithms which, as the guidance instruments themselves reach their practical performance limit, would allow for continued improvement in weapon system accuracy.

Western solid rocket propulsion technology also will be a high-priority Soviet acquisition target in the 1980s. While the Soviets have vast experience with the liquid-propellant systems which represent the bulk of their ballistic missile force, they are shifting their emphasis to solid propulsion systems, which have practical advantages over liquid systems in a variety of applications. At the same time, the Soviets have had only limited success with the progress of their solid-propulsion program. They probably will pursue the acquisition of information on solid-propellant production procedures, and propellant grain design, motor case, and rocket nozzle technologies.

The Soviets' ABM R&D effort has continued apace since the 1960s. As a result, they have gained considerable expertise in the development of large fixed-site radars for early warning, tracking, and engagement, and their interceptor technology has also improved substantially over the years. Areas remain, however, in which the Soviets will still seek and would benefit from sophisticated Western ABM technology. These include signal processing for detection, discrimination, target assignment, and sensor technology, particularly in the long-wave infrared portion of the electromagnetic spectrum applicable toward improving their launch detection capability.

Priority Soviet targets in the aircraft area will include Western materials technology, particularly composite materials to allow weight-efficient designs. The Soviets would also benefit from the acquisition of certain engine technologies, in particular those critical to the development of high-bypass turbofans for large strategic airlift type of aircraft. While, in general, Soviet avionics technology appear adequate, the Soviets have yet to demonstrate a capability to deploy reliable, accurate airborne inertial navigation systems for long-range navigation and weapons delivery. Thus, while long used in the West, these systems are still prime candidates for acquisition.

Best Available Copy

Very high priority probably will be given to the acquisition of computer-aided aircraft design technology, an area in which the Soviets are clearly impressed by US progress. In general, they also will continue to benefit from the acquisition of efficient aircraft production technology from the West to reduce costs.

While the Soviets have a strong indigenous air defense radar and missile technology, their general lag in microelectronics and microprocessing will direct them to attempt wherever possible in the West the acquisition of advanced signal-processing hardware and software.

The Soviets will continue to emphasize the acquisition of naval-related technologies applicable to improving their antisubmarine warfare capabilities, an area in which much Western technology is superior to theirs. Thus, a significant effort to acquire acoustic sensor technology can be expected, in particular that technology applicable to the development of large towed acoustic arrays that would assist the localization of Western submarines in open waters. They probably will also target the acquisition of Western signal-processing hardware and software required to fully exploit the detection capabilities of these sensors.

Another critical problem area to which the Soviets will direct acquisition is that of submarine quieting. Here also the Soviets lag the West significantly. As a result, not only are their submarines more vulnerable to detection, but the self-generated noise reduces the effectiveness of their own acoustic sensors.

An area in which the Soviets have historically lagged behind the West is precision submarine navigation—in particular, in the development of submarine inertial navigation systems. The need for improvements here will become more pressing as the Soviets develop long-range cruise missiles for land attack which require precise knowledge of launch location.

The Soviets also will continue to target technologies related to the design and construction of large aircraft carriers (for high-performance aircraft) to reduce the likelihood of poor design choices that would arise in what is for them an entirely new type of construction program.

Much of the Soviet acquisition effort in the area of tactical weapons is likely to be targeted against seeker and sensor technology for tactical missiles and precision-guided munitions. The Soviets will apply considerable effort in particular to acquiring advanced Western electro-optical technology including that related to antitank weapons. As in other weapons areas, the signal processing and microelectronics technologies supporting tactical weapon systems will also be priority acquisition targets. Technical documentation on entire weapon systems, if obtained, will be used to develop countermeasures.

In the microelectronics area the USSR is now at the stage of implementing its LSI (large-scale integration) technology to high-volume production. Despite the large acquisitions of Western technology and production equipment over the past 10 years which have brought them to the LSI level, additional acquisitions from the West are needed for the more sophisticated weapons projects of the future. Ever-increasing needs for higher precision Western equipment will extend at least through the 1980s.

In addition, the Soviets will require considerable expansion of their microelectronic material base to support continued expansion of integrated-circuit production. In this regard, the USSR is seeking Western help to build two or three poly-silicon plants that will more than double current Soviet capacity for military applications. Also, with increasing advances in the technology, the USSR already will be seeking additional Western assistance in key complementary technologies such as packaging and printed circuit board production.

The USSR is expected to focus its future acquisitions efforts on the emerging technologies related to very-high-speed integrated circuits (VHSIC) and very-large-scale integration (VLSI). It is important to note that, while VHSIC is thought of as a military development program, and VLSI as a civilian technology, there is little difference between the two as far as Soviet production needs are concerned. The same materials, production, and test equipment will be used to produce both. In both of these technological areas, the USSR has developed effective means for illegally acquiring Western advanced products.

Best Available Copy

97-341 O - 82 - 12

Prime Soviet collection efforts in computer technology through the 1980s are likely to include large-scale scientific computers such as the US-built CRAY-1 Computer. Computers of this class offer significant improvements over Soviet models in weapons-systems design and simulation and in the processing of numerical data for many military applications. Other hardware targets will include: very dense random-access memory chips; high-capacity disk drives and packs; the so-called "superminicomputer" class of machines; and the latest in general purpose computer technology. All of the above targets offer opportunities for significant performance improvements and represent technologies of substantial Soviet lag.

In computer software, the Soviets will continue to attempt to collect IBM programs and programs of other vendors written for these machines because of past Soviet decisions related to copying IBM computers. The large and growing number of IBM-compatible computers in the USSR means that collection activity in this area can be expected to increase. The compelling attraction of computer networks also should spur great Soviet interest in acquiring network-control software and other programs related to networking.

Best Available Copy

Executive Branch Comments on Testimony of Public Witnesses

Department of Defense

INSERT FOR THE RECORD									
	HOUSE / SENATE	APPROPRIATIONS COMMITTEE		HOUSE / SENATE	ARMED SERVICES COMMITTEE	X	HOUSE / SENATE	OTHER	
HEARING DATE		TRANSCRIPT PAGE NO.		LINE NO.		INSERT NO.		Committee on Science & Technology	
29 March 1982		47		1071		47A			

Comments by Witnesses

(The information follows:)

Comments on testimony of public witnesses made at hearings for members of the Committee on Science and Technology on the "Impact of National Security Considerations on Science and Technology" on March 29, 1982, as requested by Congressman George E. Brown.

The following remarks pertain to five written testimonies submitted by the following individuals: Frank Press, President, National Academy of Sciences; Robert M. Rosenzweig, Vice-President for Public Affairs, Stanford University; Robert W. Corell, speaking on behalf of the National Association of State Universities and Land-Grant Colleges; Edward Gerjuoy, speaking for the American Physical Society; and John L. McLucas, President, World Systems Division of COMSAT. In general, we agree with almost everything stated by these five witnesses. They presented a clear and dispassionate review of a very difficult and complex problem, the balance between freedom to publish on the one hand, and limiting the flow of valuable U.S.-generated technology to a potential adversary, on the other hand. The possibility of that technology being incorporated in a weapon system used against us is unfortunately very high. If the question is one of balance between these two opposed poles, then the issue is not whether but where to strike that balance.

What technical information should be published freely in our own interest, and what technical information would constitute a significant threat to national security if it reached our enemies? It is a frightfully difficult question to answer, fraught with danger not only to our whole scientific and engineering enterprise, but to our free society as a whole. It would be easier to deal with if the threat were more visible, as for example in wartime, or if there were an end in sight, but it is a question very difficult to face in peacetime and for an indefinite period. However, face it we must. Most reasonable people agree there is a real threat. None of the witnesses testified in favor of ignoring the problem or of doing nothing; they testified only in favor of giving careful considerations to any proposed restrictions. The Department of Defense has set up a DoD/University Forum with a Working Group consisting of senior University and DoD people to look at the question, and is partially supporting a study by a committee of the National Academy of Sciences, all with the intention of coming up with a sensible, workable solution with which the Universities and DoD can live.

Best Available Copy

INSERT FOR THE RECORD							
☐ HOUSE ☐ SENATE	APPROPRIATIONS COMMITTEE	☐ HOUSE ☐ SENATE	ARMED SERVICES COMMITTEE	☒ HOUSE ☐ SENATE	OTHER Committee on Science & Technology		
HEARING DATE	TRANSCRIPT PAGE NO.	LINE NO.	INSERT NO.				
29 March 1982	47	1071	47A				

Dr. Press set the scene with his statement, "The issues leading to the current controversy are not new, extending back over the past several years as public sensitivity has heightened within the United States over growing international military tensions and the increasing transfer of American technological know-how to our foreign industrial competitors." He summed up the current situation thus: "Some government officials believe that a category of unclassified research results exists whose free and open publication or dissemination, especially to particular foreign nationals, could pose an undue threat to the national interest and, at times, to national security. Accordingly, they think it is essential to control foreign access to this information. On the other hand, most scientists and engineers in academia hold that open communication is absolutely essential for a creative research environment. In their view, restrictions on scientific communication sap the strength and vitality of the edcuational and research endeavors upon which the nation's present and future technology base is founded. Moreover, such restrictions are seen as inconsistent with a free society and, in some instances, with basic constitutional rights. Neither would they like to see us forced to emulate the soviet practice of compartmentalizing and restricting access to knowledge." He then goes on the describe the NAS study which is partially funded by DoD. On the the question of issues raised by Dr. Press, that is the responsibility of the Department of State. However, the DoD has reason to be seriously concerned about certain visitors, especially from the Soviet Union, and we feel that if visits cannot be adequately controlled after such visitors arrive on our shores, than those visitors had best be kept out of the country.

Dr. Rosenzweig states: "The front line of national defense (is) science and technology . . . . If we lose that advantage over our adversaries, we would face a very substantial threat to our national security." He is concerned lest the imposition of controls have the opposite effect to that intended, namely to weaken our science by clogging the arteries of communication between scientists. We, too, are worried about that.

Dr. Corell is concerned about the effect of the new Executive Order on Scientific communications. It is true that the new Executive Order tilts toward greater care before releasing technical information, but the real crux of the matter is how it will be interpreted and implemented. We intend to do so in a reasonable manner so as not to inflict damage on the country's great scientific and engineering enterprise. Dr. Corell proposes "a thoughtful and comprehensive assessment." We hope the aforementioned NAS study will serve that purpose.

Best Available Copy

INSERT FOR THE RECORD									
	HOUSE / SENATE	APPROPRIATIONS COMMITTEE		HOUSE / SENATE	ARMED SERVICES COMMITTEE	X	HOUSE / SENATE	OTHER	
								Committee on Science & Technology	
HEARING DATE		TRANSCRIPT PAGE NO.	LINE NO.		INSERT NO.				
29 March 1982		47	1071		47A				

Dr. Gerjuoy made some very good points. To quote some of them: "As these earlier statements clearly indicate, neither the American Physical society nor I adhere to the doctrinaire view that there should be no export controls." "In the past two years, however, the federal government has been attempting to extend its export controls from well-defined categories of things to very broadly and correspondingly vaguely defined categories of scientific and technical information, termed "technical data" in the export regulations." We concur that vaguely defined categories won't do. We agree that any categories subject to export control must be clearly defined. We also know that it will not be easy to do so. Dr. Gerjuoy goes on: "The American Physical Society's position on the government's recent attempts to control the export of technical data now can be simply stated. The Society does not quarrel with the government's objective--preventing the spread of high technology which could make a significant contribution to the military potential of unfriendly nations. However, the Society does question whether the government's present approach to this objective can achieve its goal without impeding the continued progress of American science and thereby counterproductively weakening rather than strengthening this nation." He continues by commenting on the Forum which we initiated: "Because the government's attempts during the past few years to enforce the new approach to export controls have not shown much appreciation of these risks, the Society is gratified that the Defense Department recently has instituted a DoD/University Forum, composed of high-ranking DoD officials and university administrators, charged with the task of examining export controls and other national security measures affecting university scientific research and education."

Dr. McLucas makes similar points as were made by previous speakers. He emphasizes the need for clear and simple guidelines: "Once we have simple guidelines and more current information on critical technologies, industry will be able to assist government more effectively in protecting critical technologies." He goes on to warn: "If technology transfer control is important in protecting the national security, the Congress must provide the Government agencies involved in technology transfer issues with sufficient resources to consider industry requests promptly and efficiently." DoD generally concurs with these views. The real test will come when we try to promulgate specific regulations to live by.

Best Available Copy

PAPERS PRESENTED AT SYMPOSIUM ON "STRIKING A BALANCE: SCIENTIFIC FREEDOM AND NATIONAL SECURITY", 1982 ANNUAL MEETING OF THE AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE, WASHINGTON, D.C.

GOVERNMENT CONTROL OF PRIVATE IDEAS

by
Mary M. Cheh
Professor of Law
The National Law Center
George Washington University
Washington, D.C. 20052

Prepared for the Symposium on
"Striking a Balance: Scientific Freedom and National Security"
1982 Annual Meeting
American Association for the Advancement of Science
Washington, D.C.

Best Available Copy

I. INTRODUCTION

For most people science and secrecy are incompatible concepts. Scientific advance depends upon openness, sharing of ideas, and building on what has come before. Yet most people, even most scientists, would probably agree that there are circumstances in which a government might be justified in imposing secrecy on scientific research. The secrecy surrounding the United States development of the atomic bomb duirng World War II is an oft-cited case for secret science.[1/] But what if the circumstances are not quite as compelling, the context not quite as dramatic? Just how far should the government be permitted to go in limiting the free flow of scientific information?

To date government policy has generally been consistent with the view that scientific freedom -- the freedom to think, to learn, to conduct research, and to report one's findings -- is so essential to our liberty and well being that restrictions should be imposed only for the most obvious and compelling reasons. As a result secrecy restrictions have generally extended only to scientific data generated by government employees or with government money. Persons unaffiliated with the government or working independent of government support have generally been left free to report the results of their discoveries or inventions.

Unfortunately several government agencies have taken new steps to impose secrecy restrictions on private ideas -- ideas developed independent of government supervision or support.[2/] In the name of national security, these agencies have claimed authority to prevent the publication of scientific information in cryptographic research and to restrict, via export controls, the domestic dissemination of a broad range of technical data. Already the government has invoked

Best Available Copy

its authority to forbid unlicensed receipt of foreign periodicals for personal reading,[3] to attempt to bar foreign scholars from participation in university research projects or symposia, particularly in the areas of engineering and computer science,[4] to impose secrecy orders on cryptographic inventions, and to attempt to bar the publication of mathematical theories printed in foreign journals.[5] These new initiatives, combined with the government's past efforts to restrain publication of atomic energy information developed from open sources,[6] and to impose secrecy orders on and, in effect, confiscate all private inventions "detrimental to the national security,"[7] raise anew perplexing questions about the legality and the wisdom of such actions.

Scholars, academicians, and others working in a variety of fields of civilian research see the government's recent initiatives as a major intrusion into freedom of scientific inquiry and fear that more not less government regulation and control of private ideas is coming.

This article will describe the government's most recent efforts to impose secrecy controls over private ideas in the areas of atomic energy technical data and cryptography. It will examine the government's national security rationale for its actions and analyze the information controls from legal and policy perspectives. The aim is to demonstrate why these efforts, like others before, are inconsistent with freedom of speech, sound public policy, and even the government's own objectives. In concluding that there may be a very limited legal basis on which the government may impose secrecy over private ideas, the article examines why current laws and regulation authorizing government suppression of scientific research are far too broad and suggests how they may be refined and narrowed.

Best Available Copy

II. THE NATURE AND SCOPE OF GOVERNMENT CONTROLS OVER PRIVATELY GENERATED INFORMATION

A journalist writes an article about thermonuclear weapons and includes several sketches describing how a hydrogen bomb works. All of the information is acquired from public sources. The government claims the article will reveal the secret of the bomb to foreign governments or terrorists and gets a federal court to enjoin publication.[8]

A professional group of engineers and scientists holds a conference at which new results in cryptology (the study of secret messages), computer theory, or engineering will be discussed. Members, participants, and invited guests include persons from Eastern Europe, the Soviet Union, or China. The government tells the group to either bar these foreigners or risk criminal sanctions for violating export control regulations.[9]

Approximately one third of all United States graduate students in engineering, physics, and computer science are foreign nationals. The Departments of State and Commerce claim they may tell university and college officials which courses these students may attend and the areas in which they may conduct research or read papers.[10]

A professor of computer science invents a new device to encode messages and seeks a patent. Defense agency officials believe that publication of the professor's idea would be detrimental to national security. They impose a secrecy order on the invention and prohibit the professor from disclosing any information related to his new idea.[11]

All of these attempts to control privately generated ideas and to restrict the free flow of scientific information are based on statutes and regulations currently in force. These laws are not new. They are not part of a comprehensive or integrated system of information control.

Best Available Copy

They are not specifically aimed at scientists or academicians. But, taken together and read broadly, they confer a sweeping authority on government officials to regulate and suppress the communication of scientific information. This section will describe the statutes and regulations controlling privately generated information in the areas of atomic energy, technical data, and cryptology, illustrate how they have been used, and summarize the information control features they have in common.

a. Control of Atomic Energy Information

The article describing how a hydrogen bomb works was enjoined under the authority of the Atomic Energy Act.[12] Under the provisions of the Act practically all information relating to nuclear weapons and nuclear energy is designated as Restricted Data.[13] Information coming within the broad definition of Restricted Data is "born classified." It is considered to be a government secret as soon as it comes into existence. Only persons having the proper government security clearance may communicate or disclose Restricted Data, and anyone who communicates such data with reason to believe it will harm the United States or help a foreign nation may be fined or imprisoned. A person has "reason to believe" if the government advises him that it has reason to believe that communication of Restricted Data will harm the United States or help a foreign nation.

These provisions are sweeping in their reach but, in practice, their scope has been limited by several factors.[14] First the government has extended security clearances to large numbers of persons. Second it has declassified a significant amount of information otherwise falling within the broad definition of Restricted Data. Finally, and most relevant to the present discussion, it has generally applied the information

Best Available Copy

control provisions only to Restricted Data generated by government employees or under government support or sponsorship. As indicated, however, the Department of Energy recently sought and obtained judicial support for the government's long-held view that the information control provisions may be applied to any information falling within the definition of Restricted Data regardless of where the information originated.

In the government's view, Restricted Data is a government secret unless and until it has been declassified. It doesn't matter if the information is already in the public domain. It doesn't matter if the information can be derived from information already in the public domain. It doesn't matter if the person developing the Restricted Data is a scientist, an academician, or a terrorist. All that matters is that the information falls within the definition of Restricted Data, that the government has not affirmatively declassified it, and that the government believes it warrants protection in the interests of national security.

The significance of such a position should be obvious. A scientist in a university laboratory, a researcher in a private plant, or an enterprising citizen can all independently compile, develop, or invent Restricted Data. Their work is then "secret" and subject to government suppression. Of course, the government may not choose to apply the law this broadly, but it maintains that it could do so if desired. And, of course, the government has no effective means of monitoring the dissemination of all privately generated information which can be defined as Restricted Data, but selective or even random application of the law may deter large numbers of scientists and others from dealing with atomic energy information.

Best Available Copy

Whether government officials are correct in their broad reading of the Atomic Energy Act is uncertain. The Act itself does not provide a clear answer. And, although a federal district court in United States v. The Progressive, Inc.[15] agreed that the law applies to privately generated information, the case was rendered moot on appeal after the suppressed information was published elsewhere.

b. Control of Technical Data

Two statutes, The Arms Export Control Act of 1976[16] and The Export Administration Act of 1979,[17] control the export of goods from the United States and foreign nationals' access to such goods in this country. Both laws bear upon the present topic in that the regulations of each include information ("Technical Data") among the items subject to control and define export broadly enough to include the domestic publication or presentation of that information. Both laws have served as the bases for government attempts to ban foreigners from science and engineering conferences and attempts to ban foreign graduate students from college courses in physics, computer science, and engineering.

Under the Arms Export Control Act the State Department, in the interest of national security, maintains an extensive list of munitions and, by regulation, prohibits their import or export unless a license is first obtained. The regulations known as the International Traffic In Arms Regulations[18] (ITAR) broadly define technical data as "any unclassified information * * * used * * * in the design, production, manufacture, repair, overhaul processing, engineering, development, operation, maintenance, or reconstruction" of items on the Munitions List or "any technology which advances the state-of-the-art or establishes a new art in an area of significant military applicability in the United States."[19] Under ITAR, an "export" occurs not only when

Best Available Copy

technical data is actually sent out of the United States but also when American citizens travel abroad and, for example, visit plants and attend briefings and symposia. An export also occurs domestically when information is disclosed to foreign visitors and students via academic instruction, symposia or, apparently, simple publication.[20]

Under authority conferred the Export Administration Act of 1979, the Commerce Department administers restrictions on the export of goods and services from the United States.[21] In essence the export of almost all commodities, except, for example, munitions which are controlled under ITAR, is prohibited unless authorized by Commerce Department license or regulation. Under this law exports may be restricted or prohibited altogether to protect national security, to implement foreign policy (e.g. trade embargoes against the Soviet Union for the invasion of Afghanistan or against the Polish government for the imposition of martial law), or to preserve short supplies. Like the Arms Export Control Act and the previously discussed Atomic Energy Act, the Export Administration Act and its implementing regulations are sweeping in scope.

Technical Data includes "information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization or reconstruction of articles or materials" on an extensive Commodity Control List.[22] And, here again, an "export" encompasses not only an actual transmission of technical data outside of the United States but also its release orally or visually to foreign nationals in the United States or abroad.[23]

Under both statutes the definition of Technical Data is so broad and the Munitions and Commodity Control Lists so extensive, an enormously wide range of information is potentially subject to

Best Available Copy

government suppression. Scientists have concluded that export regulations extend to data such as new developments in metallurgy, signal detection techniques, algorithmms, computer technology and so forth. Indeed the potentially sweeping scope of regulations governing the export of technical data prompted a Defense Department official to say that "ITAR, if enforced to the letter, would cover virtually everything done in the United States."[24]

In practice the reach of Commerce and ITAR's sweeping information controls over technical data -- like the reach of the Atomic Energy Act's controls over atomic energy information -- has generally been limited. First the government is aware of and presumably restrained by the possibility that a broad reading of the export controls violates the First Amendment guarantee of free speech.[25] Second the government has disclaimed any desire to apply the regulations as a general monitor of academic and scientific research[26] and, in fact, no one has been prosecuted for the simple publication of scientific and technical articles containing ITAR or Commerce Department technical data. Finally, unlike the experience under the Atomic Energy Act, the application of ITAR and Commerce information controls has also been restrained by court interpretation, by a specific exemption for technical data already in the public domain, and by initiatives -- not yet final -- to tighten the language of the regulations.

In United States v. Edler[27] a corporation and its President were convicted of the unlicensed export of technical data related to articles on the United States munitions list. Without prior approval from the Office of Munitions Control, the Corporation sold its expertise in creating durable lightweight materials and carbon composites to a French firm known to produce rockets and missiles. The Ninth

Best Available Copy

Circuit Court of Appeals admitted that the language of ITAR could be read to restrict not only the export of highly technical and militarily important data but also relatively innocuous information such as the basic principles of the diesel engine. The Court nevertheless upheld the regulations against a constitutional challenge by construing them narrowly. To constitute a violation of ITAR, the Court said, technical data must relate significantly or directly to items in the Munitions Control List and, if the information has both military and civilian application, the defendant must know or have reason to know that the data was intended for a prohibited military use. The Court rejected a defense based on the public availability of the information. It noted that public availability entitled the defendant to an exemption under ITAR but ruled that the defendant was not entitled to the exemption because he failed to claim it through the administrative process.

Under both ITAR and Commerce Department regulations, publicly available information is exempt from export controls.[28] Under ITAR the public availability exemption extends to unclassified information which has been published and widely disseminated as through sale at newstands and bookstores or made freely available at public libraries. Although this exemption is an improvement over the Atomic Energy Act's silence on public availability, by itself it really offers scant comfort to scholars and academicians who publish ITAR technical data. First the exemption does not protect publication of new ideas or old ideas combined in a new way. Second, as the Edler Court ruled, even if the information is in fact widely available, the person relying on the exemption in a later prosecution must first demonstrate that he sought and obtained prior administrative approval of the exemption. The

Best Available Copy

publicly available exemption under Commerce Department regulations is a stronger protection for scientists and academicians. It provides for an automatic license for the export of "data that have been made generally available in any form," and of scientific and educational data defined as "information not directly and significantly related to design, production, or utilization in industrial processes" and "instruction in academic institutions and laboratories."[29]

The reach of both ITAR and Commerce Department Regulations may be further confined by proposed amendments. In December 1980 the State Department offered revisions to ITAR which, among other things, will apparently protect the simple domestic publication of information falling within the Technical Data definition.[30] To date the revisions have not been finally adopted. With respect to Commerce Department controls, a group of government agencies is currently putting together a "Militarily Critical Technologies List." The list will identify technology considered essential to an advanced military capability and will be used as a basis for revising the Commodity Control List. The aim is to exclude basic scientific knowledge, but there is uncertainly over whether a clear line can be drawn along these lines. This initiative, too, is yet to be completed.

Nothwithstanding these restraints on the broad language and potential reach of export regulations, recent experience shows that they still pose a palpable threat to scientific and academic freedom. As indicated, on several occasions they have been the basis of government efforts to prohibit the presentation of new research in cryptography and other technological fields and to limit foreign student access to certain technical information in university classrooms and

Best Available Copy

libraries. Furthermore, a Congressional subcommittee looking into the information control provisions of the export laws suggests that they are being used to pressure researchers into withholding publication of technical reports -- not to protect national security -- but to deny other countries the economic advantage of the information.[31]

It is small comfort to scientists and researchers to note that these actions would probably not survive a court challenge. The cost of testing the law may be too great. The scientist might lose and risk criminal sanctions. He might not want to seem uncooperative or unpatriotic. And, even for someone willing to pursue a challenge, frustration may be the only consequence as the government can always desist before matters go that far.

Right now, to be completely safe and in full compliance with the broadly written export regulations, a scientist must consider whether the publication or communication of his work includes technical data and whether it will be available to foreigners. If so he must apply to either the Office of Munitions Control or the Office of Export Administration for the requisite export license or an exemption. Under ITAR, license applications are reviewed for national security implications by defense agencies most directly concerned with the subject matter of the export and for consistency with foreign policy objectives by the Office of Munitions Control. Export licenses may be denied, revoked, suspended, or amended by the State Department without notice whenever it believes such action to be advisable in furtherance of world peace, the security of the United States, or the foreign policy of the United States.[32] Similarly, under Commerce Department regulations, all licenses and authorizations are subject to revisions, suspensions or revocation without notice at any time and shipments or

Best Available Copy

transmissions can be stopped at any point in order to prevent unauthorized exports.

c. Control of Cryptographic Information

Cryptology is the science of secret writing and cryptographic research explores and develops theories and methods for rendering messages unintelligible to outsiders. Until recently cryptography has been an almost exclusive concern of governments. But, of late, there has been an explosion of private sector interest in cryptography.[33] Widespread commercial use of computers and electronics has generated strong demand for technology to insure information security. Businesses, particularly banks and other commercial groups which rely heavily on such things as electronic fund transfers and electronic transmission of business data, are seeking security against thieves, terrorists, and competitors. Individuals are seeking privacy protection against snooping and the compromise of sensitive personal information. University mathematics, engineering, and computer science departments are devoting more of their research efforts to cryptology.

The United States government, in particular the National Security Administration, is uneasy with this explosion of private interest in cryptographic research. It fears that widespread publication of cryptological research will help unsophisticated nations beef up their code systems and thus render out ability to spy on them less effective. It also fears that publication or dissemination of research in the area may accidentally lead to a compromise of NSA designed cryptosystems.[34] For both reasons, the government has pursued a variety of strategies to slow-down, oversee, or prohibit altogether non-governmental work in cryptology.[35] These strategies have been hampered by the fact that the government has no specific statutory authority

Best Available Copy

to impose secrecy on private, as distinct from government, cryptographic research. It has, however, relied on export controls, previously discussed, and the Invention Secrecy Act of 1951.[36]

Under the Invention Secrecy Act all patent applications submitted to the Patent and Trademark Office are inspected by a special security team to determine whether they contain information possibly bearing on national security. Applications so identified are referred to appropriate defense agencies who then determine whether publication or disclosure of the patent "would be detrimental to the national security." If such a finding is made, a secrecy order is issued rendering the invention a government secret.

A secrecy order lasts for one year but it may be renewed. Indeed a number of secrecy orders have been in effect for over thirty years. Approximately three hundred new secrecy orders issue each year but most of these cover applications originating from within the government or from government sponsored contracts or research.[37]

Upon the issuance or continuation of a secrecy order, a patent applicant is criminally liable for wilful publication or disclosure of information covered by the order. Additionally the applicant loses the economic benefit of his invention. He may, however, seek "just compensation" for the damages caused by issuance of the order or as remuneration for the governments use of the invention.

The only appeal from a secrecy order lies with the Secretary of Commerce. The statute does not contemplate judicial review of any kind, although challenges to secrecy orders have reached the courts.[38] In most cases, the issues revolve around questions of patent infringement or whether and to what extent the government owed the inventor

Best Available Copy

compensation. Remarkably, however, no one has ever challenged the secrecy provisions of the Invention Secrecy Act on First Amendment grounds. Legal commentators, including a Congressional Committee, believe that the law, if so challenged, would be declared unconstitutional.[39]

In at least two instances the government has invoked the provisions of the Invention Secrect Act to suppress information about cryptographic inventions.[40] In 1977 the Wisconsin Alumni Research Foundation filed an application to obtain a patent on a new encryption or cipher device which would protect computers from penetration by unauthorized individuals. The device was developed by University of Wisconsin professor George I. Davida and his graduate assistant using advanced mathematical theories and techniques. Months later, instead of issuing a patent, the Patent and Trademark Office informed the inventor that the cipher device was protected under an Invention Secrecy Order. The order stated that disclosure of the principles involved in the device "might be detrimental to the national security" and would subject violators to criminal penalties. The local press reported on the incident and a rash of national and international publicity followed. Then, barely two months after the order was issued, it was rescinded. The order left as it came -- without explanation, elaboration, or information on its source, scope, rationale, or the procedures available to challenge it.

The director of NSA later explained that the issuance of the order was a bureaucratic error because, as it happened, the material on which the patent was based had already been published in the open literature. The NSA director blamed the error on the review procedures used and began a new procedure whereby decisions on secrecy, previously made by middle management personnel, would now be reviewed by a higher-

Best Available Copy

level committee.

In another case, three private inventors faced the same treatment when they sought a patent for a voice scrambler which would permit radio and telephone users to converse without being overheard by others. They filed their application in 1977 and six months later, instead of receiving a patent, they received a secrecy order. Then, a few months passed and the order was lifted. The NSA director acknowledged that he personally authorized imposition of the order but he declined to explain why the order had been lifted.

d. Common Features of Information Control Laws

Government secrecy controls over private ideas in the areas set out above share a number of key features which bear upon their legality, wisdom, and effectiveness.

First, the expressed rationale for the control is the protection of national security -- broadly defined to include the implementation of foreign policy objectives. Nowhere, however, are the specific interests of national security set forth, or the particular security threats identified. And in cases in which secrecy controls over private information have become public, as in the Progressive case and the cryptographic invention cases, the government has been unable to substantiate alleged threats to national security. The Progressive published its article, the inventors received patents for their inventions and no discernible harm to national security has occurred.

Second, the applicable legislation and regulations are written in vague, openended, and expansive terms. Although the government disavows use of its broad authority to suppress scientific and academic

Best Available Copy

research, it invokes such authority on occasions when convenient or politic to do so. And, although there has been no prosecution of scientists under these laws, the mere prospect that it may happen is a suppression of itself. The broad scope of the laws and regulations is the oftstated reason why many experts believe they are subject to successful constitutional challenge. At the least the courts will likely read these laws more narrowly than the agencies which administer them.

Third, these controls are arguably applicable to private information and the government has consistently maintained that they so apply. Yet, in fact, the government actually applies them almost exclusively to government generated information. Where the controls have been applied to privately generated information, the instances are few enough to suggest that the government could well live without them.

Fourth, short of court challenges to these laws -- almost never bought -- agency action is subject to no outside monitor, no review by outside experts and, until recently, very little Congressional oversight.

Fifth, within the administrative agencies themselves, the procedures for challenging agency action are either burdensome or simply unavailable or ineffective. There is no coordination among the agencies to administer information controls in a coherent, coordinated way.

Finally, the government's actual ability -- even if it had the necessary desire -- to control or monitor data published or otherwise communicated by private citizens is quite limited. Absent heavy reliance on punishment after the fact or an unprecedented system of prior review, preventing the communication of private ideas is really a hit or miss or arbitrary proposition.

Best Available Copy

III. THE NATIONAL SECURITY - JUSTIFICATION FOR GOVERNMENT INFORMATION CONTROLS _ THE ALL PURPOSE RATIONALE

On a theoretical level, at least, most scholars would agree that the government should not be powerless - even in the face of First Amendment freedoms or other claims of individual liberties, to protect our nation's security. Whether the protection of national security is the primary or most fundamental government objective is debateable, but certainly it ranks among the chief reasons why people organize in society and form governments. After all, as one Justice of the Supreme Court remarked, the protections of the Bill of Rights are not a suicide pact. Indeed national security and national defense have been among the few reasons the Supreme Court has approved governmental racial and sex discrimination.[41]

Accepting the validity of a national security rationale for governmental action does not, however, deny that claims of national security are very difficult to evaluate. A major problem is defining what we mean by national security. On the most elementary level national security means protection from physical attack or the reasonable apprehension of such attack - war, invasion, or troops poised to strike.

But national security may mean much more than this. It may be implicated in the developing economic or military strength of rival nations, in the weakness of our allies, or in our dependence on foreign supplies or economic troubles at home. More broadly, national security may be all of those strengths which make us a great nation; including the very freedoms that national security is sometimes said to be "balanced against." General Maxwell Taylor expressed the broad

Best Available Copy

notion of national security as including

> "current assets and national interests, as well as the sources of strength upon which our future as a nation depends . . .[These] range widely from political assets such as the Bill of Rights, our political institutions and international friendships, to many economic assets which radiate worldwide from a highly productive domestic economy supported by rich national resources. It is the urgent need to protect valuables such as these which legitimizes and makes essential the role of national security." [42]

But the meaning of national security, once unpinned from physical security and war, becomes hard to confine. It may come to mean so much that it means little or that it means all things to all men.

Another problem in evaluating national security justifications for information controls is that the government's specific national security interest is often left unstated or unquestioned. We are told that we believe that security matters cannot or should not be discussed openly. The phenomenon of "we can't talk about - you'll have to trust us" allows government officials to allege national security dangers in the vaguest and most general way. Outsiders are thus left to speculate about whether the dangers are real or whether the government is simply using the label of national security to relieve it of the burden of proving its assertions or, worse, using it to hide the actual weaknesses in its position. This difficulty is illustrated in the testimony of Admiral Bobby Inman, then head of the National Security Agency, before a Congressional Subcommittee of the Committee on Government Operations looking into, among other things, government secrecy imposed on private research on cryptography. Admiral Inman assured the members of the committee that secrecy was necessary but, because they were not cleared to receive classified information, he could not be more specific. [43]

Best Available Copy

Another related difficulty in evaluating national security justifications for information controls is the outsider's lack of, or perceived lack of, competence. How is a judge, a Congressman or anyone unfamiliar with the insider's view of military and diplomatic policy able to assess the risks associated with releasing particular secrets? This problem is compounded when the secret is in a highly technical or scientific field in which the outsider has little or no expertise. Some legal scholars have argued that this lack of competance should, for example, lead the judiciary to defer to the executive on so-called national security cases.[44] Others view this as an abdication of judicial responsibility. In either case the question of competence is a thorny one.

A final difficulty in evaluating a national security rationale for information secrecy is the natural skepticism, born of experience, which many people now feel toward this explanation of government behavior.

This skepticism may be part of a broader lack of faith in government officials' honesty and sincerity but it also seems directly related to the government's overuse of the national security justification. In court challenges the government has claimed a national security justification for a wide range of actions including actions against communists, aliens, politically motivated strikers, persons such as university professors whose loyalties were questioned, state governments involved in interstate conflicts, former CIA agents, newspapers publishing embarrassing information, teachers, and so on. A striking fact about some of the more celebrated national security cases involving the supression of information is how the government's claims of grave harm have not held up in retrospect. For example, it has never

Best Available Copy

been demonstrated that the publication of the Pentagon Papers in any way prolonged the Viet Nam war, resulted in the death of soldiers and government agents, or destroyed foreign alliances - all claims made by the government to stop publication. Similarly there is no evidence that any foreign nation or terrorist group has acquired a hydrogen bomb because it obtained and read the Progressive magazine article on how a hydrogen bomb works - again, a claim made by the government to suppress publication. These experiences have undoubtedly lead many to conclude that invocation of national security is the government's version of crying wolf.

Notwithstanding these difficulties, common sense tells us that there is some legitimate national security interest in controlling atomic energy information and technical data, such as crytographic data. But simply acknowledging a government interest should be the beginning and not the end of national security analysis. The further questions are: what specific harms to national security are claimed; are they grave and imminent or only slight and speculative; are the particular controls sought narrowly tailored to the harms alleged or are they broad prohibitions which harm other, equally important interests.

With respect to atomic energy information the government's national security claim is that information falling within the Restricted Data definition, if not kept secret, will enable non nuclear countries or subnational groups to acquire the atomic or hydrogen bomb. This claim may have been legitimate at one time but given the worldwide dissemination of atomic energy information - fostered principally by the United States government - it is no longer true today.[45] And even if it were true that Release of Definition would assist

?

Best Available Copy

others in the making of a nuclear bomb, the information controls under the Atomic Energy Act go far beyond suppressing design information or blueprints for atomic weapons. As mentioned, the definition of Restricted Data, in the words of one commentator, is broad enough to encompass "virtually all atomic energy information which the [government] believes warrants protection in the interest of security."[46]

Moreover, experts on nuclear proliferation agree that the obstacles preventing production of a nuclear weapon are not informational. Rather, they lie in acquiring the cadre of skilled scientists needed to reduce the information to application, building the sophisticated and expensive facilities needed for production, and obtaining the necessary plutonium or weapons grade uranium.

The Atomic Energy Act is flawed because it draws no distinction between highly dangerous or sophisticated technical data having direct military application and basic scientific or theoretical data. Nor is any recognition given to the fact that "effective technology transfer depends largely on the degree of interaction between those providing those acquiring data."[47] The least effective means of transfer is via trade exhibits, commercial literature, general publication, undocumented proposals, and sale of products without maintenance and operations data. This is where the Progressive article on the hydrogen bomb would be listed. In contrast the most effective means of transfer is via processing equipment with know-how, training in high technology areas, technical exchanges with on-going contracts, joint ventures, licenses with intensive teaching efforts, and the delivery of completely equipped production or processing facilities. If the government fears effective transfer of sophisticated and dangerous know-how and the loss of government secrets such as military weapons designs or

Best Available Copy

information as to the number and location of atomic defenses, then this is what it should prohibit. A broader law is unnecessary and harmful.

A similar situation exists with respect to government controls over privately developed technical data; that is, the government's national security interest, if it exists at all, is narrow while the controls applied to protect it are broad. Taking the case of cryptography as illustrative, the government fears that free dissemination of cryptographic research will enable other countries to strengthen their coding systems and make it harder for us to eavesdrop. A cryptology expert points out however, that this claim is overstated. Free publication will have little effect, he says, because "few are as intransigent in their beliefs as cryptographers are about the unbreakability of the cyphers they have invented or introduced."[48] They just won't change.

The government also claims that free dissimination of cryptological research will render government coding systems insecure but, in fact, the security of modern cryptographic systems depends not on secrecy over cryptographic theories but on keeping the keys to the coding system concealed.

A broader national security claim is implicit in the control of technical data and deserves mention. Knowledge is power and, in an age of conflict, competition, and scarce resources, some government administrators and policy makers believe that knowledge should be hoarded and traded on like any other commodity. This notion is sometimes expressed in terms of national security; that is national security is threatened when other countries learn "our secrets" in advanced technological fields because it enables them to compete more successfully to our economic detriment.

Best Available Copy

This kind of thinking is wrong because it mistakes the profound practical differences between controlling traffic in information and ideas and controlling traffic in commodities. It is inaccurate because it is based on the false and egotistical assumption that the United States is the world's unchallenged technological giant leading all other countries out of a great technological void. Its most serious deficiency, however, is that, if seriously used as a basis for policy or law making, it will eventually stiffle basic freedoms and stagnate and retard - not the world's technological advance - but our own.

In short, government controls over the dissemination of technical data including cryptology appear far broader than any legitimate national security need.

Best Available Copy

IV. THE CASE AGAINST CONTROLS

In considering the arguments against government secrecy controls over privately developed information, it is important to keep in mind the distinction between constitutional arguments and policy arguments. Scientists or others may feel that certain information controls are unwise, foolish, or counter productive but, if they do not offend constitutional commands, Congress is free to impose them. In that event, opponents of controls must make their case in the political arena and not in the courts.

a. First Amendment Arguments

If applicable, the First Amendment presents the chief constitutional limitation on secrecy controls over privately generated information. The initial question is whether atomic energy information or technical data such as cryptographic information is "speech" protected by the First Amendment. A few legal scholars argue that only purely "political" speech is protected, that is, speech concerned with governmental behavior, policy, or personnel but not scientific, educational, commercial, or literary expression as such. Under such a view, political opinions about nuclear disarmament come within First Amendment protections but a scientists' lecture on atomic theory does not. Most legal scholars hold a broader conception of the First Amendment contending that protected speech encompasses all expression except the few categories specifically excepted such as pornography or defamatory falsehoods.

Under both a narrow and a broad conception of protected speech, debate or discussion concerning government policy on atomic energy or cryptography would be protected by the First Amendment. The tough question, in the context of the present discussion, is whether technical data is similarly protected. Technical data is itself a broad category

Best Available Copy

of information having no precise meaning but potentially including information ranging from basic or general scientific data such as equations, formulas, theories, or models to detailed and specific designs, blueprints, or operating manuals of particular machines, weapons, equipment, or production processes.

The Supreme Court has not faced the issue of First Amendment protection for technical data but its general First Amendment jurisprudence suggests, at least, that technical data of the basic theoretical and scientific kind is included within First Amendment protections. The Court has extended these protections to so-called commercial speech (advertising) and, in dicta, to general scientific inquiry.[49] In this regard, the Court appears to view the First Amendment instrumentally -- as a vehicle in society's search for the truth and as a protection of the individual to benefit and inform the public. The fact that the speaker speaks in a commercial setting or with the intention of making a profit is irrelevant.[50]

Whether the Court would go further and find all technical data within the First Amendment is difficult to predict. On one hand, society may have as strong an interest in the free dissemination of technical data as it does in commercial information like advertising. And, as the Court has noted many times, a finding that certain communication is within the First Amendment does not mean it can never be regulated in any way.[51] On the other hand, the Court has tended to resist First Amendment innovation and has come down hard on defendants whose claims of free speech conflicted with government claims of national security.[52] Some lower courts have assumed technical data falls within First Amendment protections.[53]

Best Available Copy

If communication of atomic energy information or technical data such as cryptology is protected by the First Amendment, then restrictions aimed at the content of that communication can survive only if the government can show that it presents a clear and present danger of substantial and serious harm.[54] The test for prior restraint is even more rigorous. Prior restraints on protected speech will only be upheld if the government can demonstrate that they are necessary to prevent direct, immediate, and irreparable damage to the nation and only if the implementing law is narrowly drawn and provides for prompt judicial review.[55] If broadly read and applied, none of the statutes discussed in Section II could survive these tests.

b. Policy Considerations

Even if government controls over privately developed atomic energy information and technical data such as cryptographic research are constitutional, are they wise? Do they accomplish national security objectives? If so, at what cost to other, equally legitimate public interests? Is that cost too great?

The policy arguments in favor of unrestricted research and against government suppression of privately generated information are numerous.[56] Taken together they present a formidable challenge to practically all government restrictions on the free dissemination of nongovernmental atomic energy and cryptographic information.

First, government suppression of broadly defined categories of privately generated atomic energy information or technical data such as cryptography is practically impossible. Effective suppression would require an elaborate and costly monitoring system and -- even then -- controls would be ineffective against dissemination of information from

Best Available Copy

sources outside of the United States.

Second, the national security or economic benefits from broad controls are hard to discern or perhaps illusory. Experts tell us that control of atomic energy information will not prevent other countries from acquiring a nuclear capability; that publication of crytographic research will not enable other countries to tighten their codes or render ours penetrable; and, that in the long run, scientific protectionism will not help our economy, it will hurt it.

Third, broad controls are inconsistent with at least some of the government's own objectives. For example, while defense agencies seek to limit and censor private cryptographic research, other agencies such as the National Science Foundation fund such research and expect publication of results.

Fourth, broad controls ignore or sacrifice important non-military needs for information. It is generally known, for example, that atomic energy data is applied in the electric power industry and in the practice of nuclear medicine. Suppression retards progress in these areas and impairs the United States' ability to remain a world leader in the nuclear technology field. With respect to cryptography, nongovernmental research on codes and cipher is providing the know-how to protect the confidentiality and integrity of information stored in and transmitted from computer and electronic data banks and networks. As our society relies more and more on such information systems, technology which insures information security will become increasingly valuable. The development of such technology will also permit the United States to compete successfully in meeting the growing international demand for information security. Work in cryptography is especially sensitive to restraint since cryptosystems

Best Available Copy

must be constantly upgraded and changed as the information systems they protect change or are compromised.

Fifth, broad information controls over atomic energy and cryptographic information retard scientific progress in related fields. Research in atomic energy and cryptography has led and likely will lead to important discoveries in engineering, communications, mathematics, and computer science.

Sixth, suppression of privately generated information generates hostility and suspicion between the government and the scientific and academic communities. Already one major university has criticized State Department requests that it enforce security related restrictions on foreign scholars it has informed the Department that it will not be its policeman.

Seventh, broad controls conflict with international cooperation in scientific exchange.

Finally, several indirect but equally negative effects flow from the suppression of privately generated atomic energy information and technical data such as cryptographic information. Citizens are disabled from judging whether government policy is wise or foolish, bureaucrats can more easily hide errors and mistakes, and a precedent is created which can be used to chip away at scientific and academic freedom in other spheres.

If all of these arguments can be marshalled against the current information controls, why did Congress authorize them? In fact, Congress may not have intended any of the statutes discussed above to permit the suppression of scientific research.[57] And, even if Congress gave the matter any specific thought, it did so in the context of passing com-

Best Available Copy

prehensive laws only a few sections of which are devoted to information controls. Moreover, the relevant statutes were passed (or built upon laws passed) decades ago when circumstances and needs were quite different.

Why the current laws remain on the books is a harder question. Perhaps the matter has not received enough public attention. Perhaps the scientific, academic, and business communities have not lobbied hard enough for a relaxation of information controls. Perhaps Congress is persuaded by defense agency officials that more not fewer information controls are necessary. As already noted, national security claims are difficult to assess. Is national security really threatened or are defense agency officials overreacting? Are information controls really necessary or only administratively convenient? No one likes to err on the side of endangering national security. No one likes to be accused of aiding the enemy. Perhaps the current information controls remain because the arguments against them are complex and subtle and because, as the next section suggests, there are no easy solutions to accommodating legitimate national security concerns and free scientific exchange.

Best Available Copy

V. STRIKING A BALANCE

United States defense agencies do not appear ready to abandon efforts to control privately developed information. Indeed, they seek to broaden their powers and invoke national security as the justification. Scientists and members of the academic community view controls over privately developed information as a threat to freedom of speech and freedom of inquiry. Is there any way to strike a balance between the positions of these two groups? Is there, in other words, a way to accomodate legitimate government interest in national security and the public interest in the free exchange of ideas.

Some might argue that there is no room for accomodation, but most people who have examined the issue in the context of atomic energy and cryptography would disagree.

Several general approaches have been suggested. One is definitional, that is, we should define very specifically and very narrowly the kind of information which poses such grave national security dangers that it cannot be published and control only that. Frequently offered definitional strategies are to try to draw a distinction between basic science (e.g. laws of nature) and advanced, state-of-the-art technology (e.g. blueprints and designs) or to draw a distinction between information which has direct and critical military application and that which does not.

The definitional approach is appealing but difficult to implement. A major problem is that it is often quite difficult to draw precise lines. For example, in cryptography there is very little

Best Available Copy

difference between an algorithm and a mathematical formula and very little difference between theory and application. And, in the atomic energy area, the difficulty of linedrawing apparently led the original drafters of the Atomic Energy Act to abandon efforts to exempt "Basic Scientific Information" from the definition of Restricted Data. Other problems with the definitional approach are 1) descriptions of controlled and uncontrolled data must be frequently revised as information passes into the public domain or becomes obsolete or is surpassed and 2) even very general descriptions of data considered sensitive might of itself reveal important national security information.

A definitional strategy is currently employed in the control of technical data under the export regulations. The complaint is that the definitions of technical data are too broad and the lists to which they refer are too extensive. Efforts to tighten up the definitions include the previously mentioned government interagency development of a "Military Critical Technologies List" which will identify technology essential to an advanced military capability and revise the Commodity Control List accordingly.

Similarly, definitional solutions have been offered to deal with privately generated atomic energy and cryptographic information. For example, two Stanford Law Professors suggest that the definition of Restricted Data be amended to distinguish between "deducible" information generally available to the private thinker (information developed "from known physical principles, careful reasoning, extrapolation from demonstrated capabilities of related technologies, and the large body of general information that is already in the public domain") and nondeducible information or information deductible "only from an

Best Available Copy

elaborate experimental program of the type carried out or sponsored by the government."[58] Their specific amendment would add the following exception to the Restricted Data definition: "other than data in the public domain or data gained through research involving generally available facilities or equipment."

In the cryptology area, a report prepared for the National Telecommunications and Information Administration of the Commerce Department suggests that controls be limited to "specifications associated with products or equipment categorized as leading-edge technology, and only when these data would effectively transfer manufacturing know-how significantly superior to available foreign technology . . . scientific talks and technical publications should be avoided."[59]

Both of these definitional suggestions can be faulted as imprecise but they undeniably pare down the scope of present or requested controls and, indeed, they are far more precise than language found in a whole variety of statutes which administrators and courts have managed to apply through the years.

Another general approach for striking a balance focuses on the decisionmaker, to wit, the one who decides whether particular information should or should not be suppressed. The idea here is to acknowledge that definitional efforts will always be imperfect and that there will always be close calls and grey areas. Therefore, we should be sure that the decisionmaker is wise, fair, competent, broadminded or whatever. The possibilities include any or all of the following: decisionmaking by only "top level" officials (presumably to insure more thoughtful and considered judgment; this was a solution offered by then NSA head Inman to limit defense requested patent secrecy orders on cryptographic

Best Available Copy

inventions); decisionmaking by an intragency group (to insure a balanced view from the defense and nondefense sectors), and decisionmaking by a panel of persons inside and outside the government and with or without expertise in the area in question (to insure public acceptance, outside oversight, and an even wider range of views). Obviously, the decision-maker solution is only as good as the persons selected to decide. They may or may not be thoughtful or competent and they may or may not adequately represent the interest they are presumed to represent. Here again, though, the approach is helpful, albeit imperfect.

A third approach is to focus on the process of decisionmaking. Persons affected by adverse government action (secrecy orders, denials of license, etc.) should be given the full range of due process rights -- notice, opportunity to be heard, reasons for the action, prompt judicial review, in camera if necessary, and so on. Of course judicial review may be an unsatisfactory basis for accommodation. The approach is adversarial and a court may feel captive or unequal to the technical nature of the decisions it is asked to make.

All three approaches hold promise and should be pursued. And, it should be borne in mind, they are not mutually exclusive. Moreover, each can be strengthened by the use of presumptions and burdens. That is, for example, privately generated information can always be deemed presumptively unrestrained and the case for restraint always put on the government. This is another way of saying that all close calls will go to freedom of expression.

Once any or all of the above approaches are chosen, thought must be given to the method of implementing the choice. There are at least three possibilities: legislation and regulation, funding controls,

Best Available Copy

and voluntary cooperation. Of these, the legislative route seems preferable as it offers the greatest scope, flexibility and legitimacy.

Voluntary plans and funding controls have a number of deficiencies. A chief shortcoming is that they can only have limited impact. For example, although the government may be able to "buy up" all of the talent in very limited areas such as cryptographic research, most privately developed information will be generated without government financial help. Voluntary controls also suffer from the fact that they may breakdown at any time, they will be applied unevenly affecting only persons who choose to participate, and they may be the basis of later, hasty legislation simply because they offer a program already in place.

Legislation could combine all three approaches -- definition, decisionmaker, and process. It could narrow the reach of controls by allowing only for post publication sanctions and forbidding prior restraint. In this way, persons charged with violations will have all of the procedural safeguards ordinarily associated with criminal prosecutions.

Legislative implementation also reflects a conscious democractic choice on how to accommodate the competing interests of security and freedom and is thus more legitimate than, for example, voluntary agreements between government agencies and special interest groups. And, even if Congress delegates most of its authority to an administrative agency, it can enforce public choices through meaningful legislative oversight.

Best Available Copy

VI. CONCLUSION

The reported instances of actual suppression of basic scientific research, academic inquiry, and news media publications in the areas of atomic energy, technical data and cryptography have been few. There is no known general government policy to interfere with these endeavors. Yet, there have a number of troubling incidents which suggest that the government believes it has broad authority to control private ideas in these spheres. The mere existence of this authority and its exercise, even if only occasional, is unacceptable. It works a chilling effect on scientists and researchers in the areas in question and it sets a precedent for further controls if and when the government's voluntary hands-off policy undergoes a change.

This last concern becomes more real when one considers that over the past year, the government has moved on all fronts to restrict the free flow of information and enhance its secrecy controls. For example, the administration has introduced legislation to keep secret a whole range of information currently available under the Freedom of Information Act, the Attorney General has announced he will seek injunctions against all former intelligence agents who write books or articles without obtaining CIA clearance -- even if the articles involve no threat to national security, and the administration is supporting the most punitive version of legislation which will make it a crime for the press to identify an intelligence agent or his source -- even if the agent's name comes from public sources and even if the agent is violating federal law or agency regulations. While, again, there is no evidence that any of these decisions are part of a coordinated new policy, there is evidence that the current administration, when faced with policy alternatives, will favor censorship and control over the free flow of ideas and information.

Best Available Copy

The irony of the situation involving the government's broad controls over private ideas in the areas of atomic energy, technical data, and cryptography is that they are unnecessary and even harmful to legitimate national security concerns. Suppression generates hostility and mistrust, invites legal challenge, and neglects a broader conception of national security which recognizes that unfettered scientific research benefits us all.

Happily, there are ways to accommodate legitimate national security needs and the free flow of scientific information. Congress must, however, take the initiative and show the courage and wisdom to strike the appropriate balance.

Best Available Copy

FOOTNOTES

1. Not everyone agrees that even this effort justified the extensive secrecy system the government put in place.

2. This article will not discuss the scope of the government's authority to impose secrecy on its own information. Rightly or wrongly, such secrecy has long been accepted as a necessary corollary to the effective and efficient discharge of government responsibilities, particulary in the military and diplomatic spheres.

3. See N.Y. Times, July 15, 1981, at A22, col. 4.

4. See N.Y. Times, November 27, 1981, at A1, col. 4.

5. See H.R. REP. NO. 34, 96th Cong., 2d Sess. (1980) (hereafter "House Report").

6. United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

7. House Report, supra, note 5, at 1-25.

8. United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979).

9. See e.g. "Cryptology: Scientists Puzzle Over Threat To Open Research, Publication" Science, September 30, 1977, at 1345

10. See, e.g., N.Y. Times, November 27, 1981, at A1, col.4

11. House Report, supra, note 5, at 21-24.

12. 42 U.S.C.§§ 2011-2296 (1976)

13. Restricted Data is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category..." Although this definition appears specific, it is fraught with imprecision, primarily because of the word "concerning", meaning "related to" or "about" atomic weapons or special nuclear material. The Act defines an atomic weapon as "any device utilizing atomic energy... the principal purpose of which is for use as, or for development of a weapon, a weapon prototype, or a weapon test device." Special nuclear material is "plutonium, uranium enriched in the isotope 233 or in the isotope 235...or...any material artificially enriched" by plutonium or uranium 233 or 235. Other component parts of the Restricted Data concept have a similarly broad sweep.

Best Available Copy

The word "design," for example, includes "(1) specifications, plans, drawings, blueprints, and other items of like nature; (2) the information contained therein; or (3) the research and development data pertinent to the information contained therein," and "research and development," in turn, includes" (1) theoretical analysis, exploration, or experimentation; or (2) the extension of investigative findings and theories of a scientific or technical nature into practical application for experimental and demonstration purposes, including the experimental production and testing of models, devices, equipment, materials, and processes."

14. See Cheh, "The Progressive Case and the Atomic Energy Act: Waking To the Dangers of Government Information Controls," 48 GEO. WASH. L. REV 163 (1980) (hereafter cited as "Cheh")

15. 467 F. Supp. 990 (W.D. Wis. 1979).

16. 22 U.S.C. § 2751 et seq. (1979).

17. 50 U.S.C. App. A § 2401 et seq. (1980).

18. 22 C.F.R. § 121.01 et seq. (1980).

19. 22 C.F.R. § 125.01 (1980).

20. 22 C.F.R. § 125.03 (1980).

21. 15 C.F.R. § 370.01 et seq. (1980).

22. 15 C.F.R. § 379.1 (1980).

23. Id.

24. See Science, May 1, 1980, at 523-526.

25. In 1978 the Justice Department prepared a Memorandum directed to Presidential Science Advisor Frank Press in which the Department concluded that, ITAR, if broadly applied, are unconstitutional.
Hearings on the Government's Classification of Private Ideas Before a Subcommittee On Government Operations 96th Cong., 2d Sess. 268-284 (1980) (hereinafter "Hearings")

26. See Science, May 1, 1980, at 523-526.

27. 579 F. 2d 516 (9th Cir, 1978).

28. 15 C.F.R. § 379.3; 22 C.F.R. § 125.11.

29. 15 C.F.R. § 379.3.

30. 45 Fed. Reg. 83970 (Dec. 19, 1980).

Best Available Copy

32. See House Report, supra, note 5.

32. 22 C.F.R. § 123.05.

See Kahn, " The Public's Secrets," The Progressive, Nov. 1980, at 27-31.

34. See, "Report of the Public Cryptography Study Group," American Council on Education, Washington, D.C., Feb. 7, 1981.

35. For example, NSA was successful in getting a professional education group to agree to recommend a voluntary system of prior review of cryptology manuscripts. Id.

36. 35 U.S.C. § § 181-188 (1970).

37. See House Report, supra, note 5, at 17-18.

38. See, e.g., Halpern v. United States, 258 F.2d 36, 38-39 (2d Cir. 1958).

39. See House Report, supra, note 5.

40. Id.

41. Korematsu v. United States, 323 U.S. 214 (1944)(wartime internment of U.S. citizens of Japanese ancestry).; Rostker v. Goldberg, ___U.S.___(1981)(draft registration for men only).

42. Taylor, "The Legitimate Claims of National Security," Foreign Affairs, at 577, April 1974.

43. Hearings, supra, note 25, at 424.

44. See Edgar & Schmidt, "The Espionage Statues And Publication of Defense Information," 73 COLUM. L. REV. 929, 933(1973); But see Cheh, supra, note 14, fn. 258 at 202.

45. See Cheh, supra, note 14, at 202-207.

46. Green, "Information Control and Atomic Power Development," 21 LAW & CONTEMP. PROB. 91, 92(1956).

47. U.S. Dept. of Commerce, 116th Report on U.S. Export Controls to the President and the Congress, Appendix D, at 133-34(1977). See Gustafson, intra note 56.

48. Kahn, "The Public's Secrets," The Progressive, at 31, Nov. 1980.

Best Available Copy

49. See, e.g., Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976).

50. Id.

51. Id.

52. E.g. Snepp v. United States, ___U.S.___, 100 S. Ct. 763 (1980); Haig v. Agee, ___U.S.___; ___S.Ct.___ (1981).

53. United States v. Edler, 579 F. 2d 516 (9th Cir., 1978); United States v. Van Hee, 531 F.2d 352.(6th Cir, 1976)(by implication).

54. See, e.g., Brandensburg v. Ohio, 395 U.S. 444 (1969).

55. E.g., New York Times Co. v. United States, 403 U.S. 713 (1971).

56. See, e.g., Cheh, supra, note 14 at 202-208; Davida, "The Case Against Restraints on On-Governmental Research in Cryptography". A minority report to the "Report of the Public Cryptology Study Groups," American Council on Education, Washington, D.C., February 7, 1981; Gustafson, "Selling The Russians The Rope? Soviet Technology Policy and U.S. Export Controls," Rand Corporation Study (1981); Hearings, supra, note 25, at 406-410 (statement of David Kahn).

57. Hearings, supra, note 25, at 268-284.

58. Id at 531-541.

59. U.S. Dept. of Commerce, "Impacts of Federal Policy Options For Non Military Cryptography," June, 1981.

Best Available Copy

ACM President's Letter
February 1982

This is the text of the President's Letter for the *Communications of ACM*, February 1982.

A SCIENTIST'S VIEW OF GOVERNMENT CONTROL OVER SCIENTIFIC PUBLICATION

Peter J. Denning

This essay is based on my remarks at a session entitled "Striking a Balance: Scientific Freedom and National Security," on January 7, 1982, at the annual meeting of the American Association for the Advancement of Science (AAAS). Other members of the panel were: Mary Clak, professor of law at George Washington university; Harold Green, attorney and professor emeritus of law at George Washington University; Bobby Inman, Deputy Director of the CIA; Daniel Schwartz, attorney and former counsel to the National Security Agency; and Congressman Paul McCloskey (California).

Although my remarks are directed toward an issue before the U.S. Government, the principles herein apply in every country.

Best Available Copy

A new kind of protectionist mood is growing in Government. To reduce the risk that an open scientific discovery might harm the national security or help a foreign country close a commercial gap, the U.S. Government seeks to apply export control laws to all forms of scientific publication, whether verbal or written. Some examples:

- Early in 1980 the Commerce Department instructed the organizers of a symposium on bubble memories, sponsored by the American Vacuum Society, to disinvite delegations from Eastern bloc countries and China. After the State Department intervened, Commerce allowed the Chinese to come but required them to sign nondisclosure agreements.

- The Government proposes to restrict research assistantships in Universities to US citizens only.

- In 1978 the Government slapped secrecy orders on two applications for patents on cryptographic devices by computer scientists, but later withdrew the orders. The National Security Agency (NSA) attempted to prevent disclosure of new results at an IEEE symposium in 1980, but later desisted. The NSA also attempted to get NSF to ~~cede~~ abdicate responsibility for funding cryptographic research to NSA. At the NSA's request the Public Cryptography Study Group was formed; this group has since made a recommendation for a voluntary system of prepublication review of papers having anything to do with cryptography.

- The Government was seriously considering including software technology and software project management on the Militarily Critical Technologies List (MCTL). (Until the MCTL is published, we won't know the outcome.)

Best Available Copy

- A bill [H.R. 109] was introduced in the current session of Congress that would extend the "born classified" concept of the Atomic Energy Act to all categories on the Militarily Critical Technologies List. It would give the Government the power to prevent publication of materials deemed threatening to the national interest. (See *Communications of ACM*, July 1981, page 409.)

The export control laws are an attractive vehicle for extending the Government's protective influence because it is easy to argue that publication in international journals is a form of export. This line of reasoning is worrisome.

Because our military strength and commercial edge depend so strongly on computing, it is impossible for the computing community to avoid this issue.

Secrecy vs. Openness

Two strong principles seemingly clash on this issue: the goal of a strong national security and the goal of the free and open market. In fact, these principles are compatible. The true clash is between secrecy and openness. With few exceptions, scientific research is most likely to strengthen the national security if it is open.

There is needed a clear evaluation of the costs of achieving these goals with and without Government control of scientific publication. (Except for atomic energy, Government does not now control scientific publication.) I argue that the cost to our economic power that would be wrought by successful control on the free flow of scientific information is far greater than any reduction in risk to national security that might result from such controls. In an article for *Technology Review*, October 1981, Edward Teller argues that the limitations we impose on ourselves by restricting information are far greater than the advantages gained by others in copying our ideas.

Best Available Copy

How much control would Government have to exert over scientific publication to achieve a significant reduction in risk to the national security? It would be considerable. Far-reaching measures would be required to completely screen all items submitted to conferences or journals because of the many referees involved. Informal distribution of unpublished technical reports would have to be monitored. Scientists (and engineers) would have to obtain licenses to travel abroad to give talks or present papers. Noncitizens would be carefully screened before being allowed to scientific meetings, research labs, or universities. These measures would have to be applied uniformly toward *all* countries to effectively reduce information flow to the few who threaten our security. The required system is clearly more compatible with a dictatorship than a democracy. It would not obtain the cooperation of scientists. It would discourage young people from entering scientific careers.

Such extremes would produce side effects whose cost exceeds the benefits of the measures themselves. Scientific secrets do not keep. By depriving ourselves of efficient access to scientific knowledge, we would undermine the central reason for our technical leadership over those who threaten our security. Moreover, major efforts at scientific secrecy would harm relations with our allies, among whom cooperation is important in a troubled world. As in atomic energy, security regulations would drive wedges between civilian and military research, limiting the effectiveness of both.

The "born classified" principle worked in the area of atomic energy because the small nuclear science research community that existed around 1940 voluntarily agreed to secrecy as part of the war effort. The Government has controlled all research in nuclear energy ever since. Other countries have done likewise.

Best Available Copy

The rest of science cannot be retrofitted for the born classified principle. As noted above, our citizens are not likely to cooperate. Even if they did, other countries are not likely to follow our lead and subject their computing research to such controls. (Would we eventually plan *import* controls to keep foreign ideas out?)

Free exchange of scientific ideas is an essential part of technology transfer. New ideas reach industry directly, through our many journals, and indirectly, through the students who take them from classroom to employer. The economic leadership of the U.S. is in no small measure attributable to the most effective system of technology transfer in the world. A policy of secrecy would seriously weaken this system.

To maintain our security and economic leadership, we must promote free exchange of ideas, promote effective technology transfer, and promote public support for science. This can be done only through a policy of openness – the current policy.

In short, stanching scientific idea-flow is far more likely to hurt the national security than to aid it. Openness expedites technology transfer and strengthens our economy; secrecy confines expertise and stifles innovation. Openness encourages cooperation; secrecy breeds conflict and distrust. Openness lowers public fears of science; secrecy raises fears.

In Search of a Solution

I have heard suggestions that the potential conflict between the Government and the scientific community could be avoided by keeping defense-related research out of universities. I don't see how this could work. The Defense Department has keen interest in computer research, it has money, and it can find much of the needed expertise in universities. Moreover, as has been well illustrated with cryptography, many problem areas arising in civilian computing also arise in military computing. It

Best Available Copy

therefore seems unrealistic to hope for complete separation between civilian and military research.

Should we educate non-U.S. scientists by admitting them as graduate research assistants in our universities? Assuredly yes! Those who regard foreign students as threats to security should reflect that these students contribute to *our* body of knowledge while on our soil. Half-joking, Bob Hope once used to remark that our space program was better than our competitor's because our German scientists were better than their German scientists. The surest path to success is to get the smartest people working *for* you.

It is no accident that the computing field has been free of Government regulation *and* has an impressive record of accomplishment. The U.S. scientific community has a proven record of success in promoting national interests. Government intervention to reduce risks to the national security would upset this system, reduce its effectiveness, create friction with the scientific community, and would not work. This is why I believe that control over scientific publication would not significantly reduce risk to the national security but would exact a significant cost on technology and science. Edward Teller says, "secrecy is the road to nowhere."

If you want to win the Indianapolis 500 Mile Race, you build the fastest car. You don't throw nails on the track.

Best Available Copy

INFORMATION CONTROL UNDER THE ATOMIC ENERGY ACT

Harold P. Green*

More than 35 years ago, Congress enacted as part of the Atomic Energy Act of 1946 a provision frankly headed "Control of Information." Section 10 of the Act explicitly stated the policy that the Atomic Energy Commission "shall control the dissemination of restricted data in such a manner as to assure the common defense and security." The statutory definition of "restricted data" was all-encompassing, and was sufficiently broad to include any and all information concerning atomic energy that was not declassified by an affirmative AEC determination that the information "may be published without adversely affecting the common defense and security."

The intention of the authors of this provision was clear. In their book, The Control of Atomic Energy, published in 1948, James Newman and Byron Miller, who as principal members of the legal staff of the Senate Special Committee on Atomic Energy played a major role in drafting the Act, stated in discussing the restricted data definition:

> "These categories cover a very large area of nuclear science and embrace much that is of general importance to fundamental as well as to applied research. It does not matter whether these data are discovered or compiled in a government laboratory or in connection with the private research of an individual scientist . . . ." (p. 15).

---

* Professor Emeritus, The George Washington University National Law Center

Partner, Fried, Frank, Harris, Shriver & Kampelman
Suite 1000, 600 New Hampshire Avenue, N.W.
Washington, D.C. 20037

Best Available Copy

> ". . .If the Act does not restrict the liberty of scientific thought, it without question abridges freedom of scientific communication. The controls on information were deliberately designed to regulate the interchange of scientific ideas; to prescribe when and how a scientist may publish or otherwise communicate the results of his work . . . . Even those data describing the phenomena and laws of the visible universe are under interdict . . . ." (p. 208)

The provisions of the 1946 Act were carried over into the Atomic Energy Act of 1954 in essentially the same form, and they remain in effect to this date.

The statutory language of the Act, standing alone, easily supports the Draconian interpretation advanced by Newman and Miller, and this interpretation is further supported by the legislative history. Moreover, the Atomic Energy Commission and its successors (the Energy Research and Development Administration and the Department of Energy) have always proceeded on the basis of such interpretation. For example, in 1955 hearings before a Senate committee, William Mitchell, AEC's then general counsel, asserted that AEC had the statutory authority to compel a scientist, who had had no access to restricted data from within the government program, to submit to government security requirements, or otherwise to cease the research, if it involved information regarded by AEC as restricted data.

Although, as I have noted, this interpretation seems clearly to be supported, and probably correct, as a matter of statutory construction, it does raise questions of constitutionality under the First Amendment. The power of the government to control the dissemination of information tantamount to the power to impose previous restraints upon the communication of information. As a matter of constitutional doctrine the government bears an extremely heavy burden of justification for any such previous restraints.

There are a number of instances of public record in which the restricted data provisions of the Act have been invoked for the purpose of suppressing research or publication.

With respect to publication, the AEC in 1950 threatened injunctive action to compel Scientific American to suppress publication of an article by Hans Bethe, for which type was already set, on thermonuclear weapons. Litigation became

Best Available Copy

unnecessary when Scientific American capitulated, and AEC security officers confiscated the material in print and destroyed the plates. Then, in 1979, the Department of Energy initiated court action to suppress the publication of Howard Morland's recipe in The Progressive for building a hydrogen bomb.

In 1967, the AEC forced a number of companies to terminate private research and development programs then underway, without government funding, with respect to use of gas centrifuge technology for enrichment of uranium.

And, perhaps most significantly, later in 1967 the AEC formally proposed to promulgate new rules and regulations that would explicitly require any person who developed restricted data to apply for an "access permit." Although the proposal was not explicit on this point, if such an application were denied, the applicant presumably would not be permitted to have access to the information he had developed. Beyond this, the proposed rules provided for a new category to be known as "private restricted data" embracing any restricted data "generated, acquired, used, or possessed" outside government programs concerning nuclear weapons, gas centrifuge, gaseous diffusion technology, and naval propulsion reactors. In Orwellian, or at least "catch-22" style, the proposed rule would have prohibited any person possessing private restricted data from communicating it to anyone without first obtaining a "dissemination permit" identifying the persons to whom dissemination would be authorized and the reasons for the proposed dissemination. At the other end of the communication transaction, no one could have access to private restricted data without a "private restricted data access authorization" which would be granted only to persons identified in a dissemination permit. It was contemplated that dissemination permits and private restricted data access authorizations would be sparingly issued. Indeed, the proposed rules explicitly stated that dissemination permits would not be issued at all with respect to nuclear explosives and gas centrifuge technology.

The effect of the proposed rules would have been to prohibit all sophisticated, private research in the nuclear explosive and gas centrifuge enrichment technologies by totally prohibiting dissemination of, and access to, information that AEC regarded as classified. And in the other areas of private restricted data where research would not have been totally prohibited, dissemination of and access to information would be sharply limited by sparing issuance of dissemination permits, and research would be drastically curtailed.

Best Available Copy

These proposed regulations were published in the Federal Register for public comment on May 2, 1967 and on December 28, 1967 were republished in revised form for further public comment. Some of the particularly objectionable features I have just described were eliminated in the December version, and I am happy to be able to report that the AEC ultimately dropped the entire scheme to bring private restricted data within affirmative regulatory controls. Nevertheless, the statutory power on which the proposed regulations were based remains on the books.

The fact of the matter is that, so far as I am aware, the Atomic Energy Act represents the first and the only legislation enacted in the history of the United States explicitly authorizing government officials to control the dissemination of information. In 1958, a committee of the House of Representatives that had considered the Atomic Energy Act as a prototype for what became the National Aeronautics and Space Act of 1958 issued a report in which it characterized the information control provisions of the Atomic Energy Act "however well-intentioned, however loosely or intelligently enforced . . . a latent danger to the life of this democracy." It is a dangerous precedent, standing largely unchallenged as the law of the land for more than 35 years.

I have always been surprised about the sudden discovery in a Progressive case, or in a flap such as that involving cryptographic research, of so-called novel or unprecedented efforts by government officials to interfere with private research and publication. The precedent, the latent danger, has been there for 35 years. Newman and Miller wrote about in their book in 1948; the Scientific American episode was discussed in the press in 1950; the American Civil Liberties Union submitted critical comments on the AEC's proposed rules in 1967; I have discussed the question in several articles in numerous publications, including the Bulletin of the Atomic Scientists. Nevertheless, the American scientific community, the civil liberties establishment, and, indeed, even American industry which from time to time has suffered suppression of research, have remained anaesthetized and acquiescent in the face of this latent danger.

Let me offer a few observations as to why this threat to scientific research and free publication has survived without opposition for more than 35 years.

First, the AEC, ERDA, and DOE have generally administered their classification and security programs in an enlightened and restrained manner. They have not attempted to treat the contents of physics and chemistry books as restricted data,

Best Available Copy

and they have, until the Progressive case, shrunk from provoking a direct confrontation and legal test with respect to enforcement of the information control provisions.

Second, American industry which had had the largest economic stake in the issue, has consistently shrunk from contesting the imposition, however costly, of AEC, ERDA, and DOE information controls. In part this reflects a desire not to appear unpatriotic, and in part it reflects a realistic appraisal that industrial, profit-oriented research might not prevail in constitutional litigation against what would be characterized as important national security considerations.

Third, for many years the AEC and the Joint Congressional Committee on Atomic Energy (JCAE) cooperated symbiotically to maintain a virtual monopoly over public policy decision-making with respect to atomic energy. A major part of this cooperation involved the effort to minimize and suppress controversy. Major public policy issues were generally argued and resolved behind closed doors and rarely surfaced to full public view. This generally detracted from public interest in atomic energy issues and to a willingness to accept the "big brother knows best" approach. The information control scheme was generally protected and nourished by the JCAE because it operated to keep other members of Congress and other congressional committees from poking around in the sacred atomic energy preserve.

Perhaps with the de-mystification of atomic energy, its current involvement in bruising battles in the political arena, and the departure from the scene of the single-minded AEC and JCAE, the time has now come for constructive action to curb the scope of the atomic energy information control structure.

Best Available Copy

NATIONAL SECURITY AND TECHNICAL INFORMATION

by

Admiral B. R. Inman

Deputy Director of Central Intelligence

7 January 1982

Best Available Copy

This symposium is an appropriate place, I believe, to lay out some thoughts that all of us--scientists and public servants--should consider. These thoughts, as well as the ensuing dialogue today and later, will help us recall how much we have in common and also help us remember that national security and scientific interests can best be advanced through a joint effort. The fact is that we do have a substantial amount of common ground and experience--both in our separate fields, and in our joint work, to protect this nation and to further science.

Throughout the world today, every nation's progress and security are tied up with science and technology. Some would say that fact is a curse of the modern age; others would say it is our salvation. Technical information has given us the means to destroy civilization or, at least, revert it to the Dark Ages. At the same time, science and technology have made life safer and bountiful, given us tools to understand better the universe in which we live, and provided the weapons and intelligence systems to help us defend our nation.

There is an overlap between technical information and national security which inevitably produces tension. This tension results from the scientist's desire for unconstrained research and publication, on the one hand, and the federal government's need to protect certain information from potential foreign adversaries who might use that information against this nation. Both are powerful forces, thus it should not be a surprise that finding a workable and just balance between them is quite difficult. But finding this balance is essential, for we must simultaneously protect the nation and protect the individual rights of scientists--both as academicians and citizens.

Best Available Copy

This tension is accentuated when scientists are employed by the federal government directly, or work for the government indirectly in their own offices with federal research funds. Some of this work is done on subjects which directly affect the nation's security--e.g., its defense, diplomacy, and intelligence efforts. The federal government has always conducted these activities on behalf of our society for several reasons. It is far more convenient for the federal government to provide for the common good. Irreversible and significant harm--to the nation as a whole, and to its citizens--often is threatened and this fact is a stimulus for the federal government to act.

There are cases where interplay has occurred between science and the national security interests. One of the most obvious, of course, is the Manhattan Project of World War II in which the first nuclear weapons were created and tested. Another is the development of "national technical means" to monitor foreign compliance with international arms control accords. Science and national security have a symbiotic relationship--each benefitting from the interests, concerns, and contributions of the other. In light of the long history of that relationship, the suggestion is hollow that science might (or should somehow) be kept apart from national security concerns, or that national security concerns should not have an impact on "scientific freedom."

The need in today's world for protection of some information, for secrecy is clear--I believe--to any fair observer. Protection of the information necessary to safeguard our society, and to conduct our international affairs, must occur. Within the federal government, there is a system established by Executive Order to assess the expected damage, should certain information come into the hands of foreign enemies, and--based on that assessment--to control

Best Available Copy

access to that information so as to prevent any such exposure. This exposure potentially could occur through public release of the data, or from the successful clandestine activities of the agents of foreign intelligence services.

And we should make no mistake, foreign intelligence services--among other entities of foreign governments--are collecting all types of information in the U.S. Specific data on technical subjects is high on the wanted list of every major foreign intelligence service and for good reason. The U.S. is a leader in many--if not most--technical areas, and technical data can enhance a nation's international strength. In terms of harm to the national interest, it makes little difference whether the data is copied from technical journals in a library or given away by a member of our society to an agent of a foreign power.

A different source of tension arises when scientists, completely separate from the federal government, conduct research in areas where the federal government has an obvious and preeminent role for society as a whole. One example is the design of advanced weapons, especially nuclear ones. Another is cryptography. While nuclear weapons and cryptography are heavily dependent on theoretical mathematics, there is no public business market for nuclear weapons. Such a market, however, does exist for cryptographic concepts and gear to protect certain types of business communications.

Research into cryptography is an area of special, long-standing concern to me. When I was Director of the National Security Agency, I started a dialogue to find a common ground regarding cryptography between scientific freedom and national security. Considerable effort has gone into that dialogue,

Best Available Copy

by both scientists and public servants, and I think the results so far have been reasonable and fair. Cryptologic research in the business and academic arenas, no matter how useful, remains redundant to the necessary efforts of the federal government to protect its own communications. I still am concerned that indiscriminate publication of the results of that research will come to the attention of foreign governments and entities and, thereby, could cause irreversible and unnecessary harm to U.S. national security interests.

There are, in addition, other fields where publication of certain technical information could affect the national security in a harmful way. Examples include computer hardware and software, other electronic gear and techniques, lasers, crop projections, and manufacturing procedures.

I think it should also be pointed out that scientists' blanket claims of scientific freedom are somewhat disingenuous in light of the arrangements that academicians routinely make with private, corporate sources of funding. For example, academicians do not seem to have any serious difficulty with restrictions on publications that arise from a corporate concern for trade secret protection. The strong negative reaction from some scientists, over the issue of protecting certain technical information for national security reasons, seems to be based largely on the fact that the federal government, rather than a corporation, is the source of the restriction. Yet this would presume that the corporate, commercial interests somehow rise to a higher level than do national security concerns. I could not disagree more strongly.

'Scientists and engineers have served our society spectacularly in peace and war.' Key features of science--unfettered research, and the publication of the results for validation by others and for use by all mankind--are essential

Best Available Copy

to the growth and development of science. Both our national security and our economic development rely heavily on these features. Restrictions on science and technology should only be considered for the most serious of reasons.

But nowhere in the scientific ethos is there any requirement that restrictions cannot, or should not--when necessary, be placed on science. Scientists do not immunize themselves from social responsibility simply because they are engaged in a scientific pursuit. Society has recognized over time that certain kinds of scientific enquiry can endanger society as a whole and has applied either directly, or through scientific/ethical constraints, restrictions on the kind and amount of research that can be done in those areas. The fact is that restrictions exist today on science and technology; for example, in conducting medical experiments on human subjects, in safeguards on handling and storing radioactive materials, in controlling some research on gene-splicing, in protecting proprietary manufacturing processes, and in requiring peer review before publication of the results of scientific research. Some of these restrictions are common sense, some are federal requirements, some are simply good business, and some are good science.

Moreover, in 1952 Congress gave an example of its willingness to act when it passed the Patent Secrecy Act. This law directs procedures to ensure that public disclosure of inventions, which would be detrimental to the national security, does not occur. Such inventions are secret and are afforded appropriate protection. Equally important, this law is not totally one-sided in favor of government. The law established appeal procedures and a mandatory review process. Little use of this law has been necessary, except in the last few years and then not for long. The law is obviously not popular with all whom it regulates, but it has for thirty years now provided a precedent for a legislative solution to

Best Available Copy

the question of private versus public interest.

One sometimes hears the view that publication should not be restrained because "the government has not made its case," almost always referring to the absence of specific detail for public consumption. This reasoning is circular and unreasonable. It stems from a basic attitude that the government and its public servants cannot be trusted. Specific details about why information must be protected are more often than not even more sensitive than the basic technical information itself. Publishing examples, reasons, and associated details would certainly damage the nation's interests. Public review and discussion, of classified information which supports decisions, is not feasible or workable.

In contrast, it is a fact that in today's world Congressional reviews of sensitive Executive Branch decisions are feasible and workable. The existence, and the processes, of such reviews are intentional. I do not think it is harmful to recognize that the federal government--particularly its intelligence agencies--have in fact made mistakes in the past on occasion, and suspicion of the actions of the federal government in this regard is understandable if not always supportable. The dominant fact of this new decade is that there now exists in the Congress a forum where assertions by the government of secrecy needs can and have been challenged and examined in a properly secure environment.

I recognize that there is concern in some circles that the suspension of publication of some information, for national security reasons, means that such information will never be published. The fact is, however, that national security concerns to protect information will not--and do not--last forever. The federal government's structure and procedures, though conservative and imperfect, do work. Sensitive information does get released in due course.

Best Available Copy

The Executive Order I mentioned earlier, which requires protection of information through classification, also requires the eventual declassification of that same information. For example, voluminous classified data from World War II has been declassified and released--including intelligence materials which had extraordinary sensitivity when they were acquired. Much of the stimulating effort for computer science in this country came from government sponsored and controlled classified activity. There is in our society a legitimate need and desire which I accept that history, whether political or scientific, will be served eventually--even if national security requires that public disclosure, and personal recognition, have to be postponed.

Rather than a confrontation between national security and science, I believe that a wiser course is possible and that our joint search for that course ought to be one of our goals. A potential balance between national security and science may lie in an agreement to include in the peer review process (prior to the start of research and prior to publication) the question of potential harm to the nation. The details of such a system would have to be resolved, of course, but cooperation will be better for all of us than confrontation. Included in such a system should be goals to simultaneously preclude harm to U.S. national security and to impose no unreasonable restrictions on scientific research, publication, or the use of the results. And when restrictions are judged necessary, speedy procedures for appeals, review, and appropriate compensation should be included. One example of this type of process is that recommended in the Public Cryptography Study Group. It is not easy to create workable and just solutions that will simultaneously satisfy the wide-ranging needs of national security and science, but I believe it is necessary before significant harm does occur which could well prompt the federal government to overreact.

Best Available Copy

SCIENTIFIC FREEDOM and NATIONAL SECURITY

A Case Study of Cryptography

by

Daniel C. Schwartz

(Partner; Bryan, Cave, McPheeters & McRoberts;
Washington, D.C.*)

Before the Symposium entitled
"Striking a Balance: Scientific Freedom and National Security"
American Academy for the Advancement
of Science
Annual Meeting; Washington, D.C.
January 7, 1982

*Former General Counsel,
National Security Agency

Best Available Copy

In April 1981, the National Security Agency ("NSA") agreed to the proposal of the so-called Public Cryptography Study Group to establish a formal, voluntary pre-publication review procedure for learned writings in the field of cryptography. The events that led to the establishment of that process, and the forces that continue to influence it, provide a unique opportunity to consider the interplay between scientific and academic freedom, on the one hand, and national security issues, on the other. I will discuss today how these issues developed and will give my perspective on the lessons learned from this experience.

Initially, I should disclose that for a period of two years from October 1979, I had the pleasure and honor of serving as NSA's General Counsel. In that position, I was closely involved in developing and participating in the Agency's actions and responses with regard to various questions as they pertained to the academic community. I also served as the Agency's representative on the Public Cryptography Study Group, participated in drafting its positions (along with the other members of the Study Group), and voted in favor of its conclusions, along with all but one of the Study Group's members.

In October of last year, I returned to the private practice of law, after a total of eight years in two different government agencies. I am presenting here my personal views, albeit undeniably influenced by my years of public service.

Best Available Copy

The initial question that had to be answered was: Is there really a problem? That is, is there a serious, potential impact on the security of the nation if scientific works relating to cryptography are published? This question is somewhat easier to comprehend in other contexts. Thus, even though such questions remain controversial, it is easier for persons to at least understand how there could be a problem if secrets of the atom bomb are revealed, or highly sophisticated computer technology is transported to the Soviet Union or the Third World. The question as it is addressed to cryptography is more difficult to discuss in a specific, tangible way.

We have matured past the time when we considered it ungentlemanly to read other people's mail: it is recognized that the United States has an active effort in both securing many of our own official communications and in producing intelligence from foreign communications. The examples of the importance and effectiveness of these efforts are many. Unfortunately for our purposes here, everything that is very recent remains classified, although major achievements from the time of World War II have now become known: the Allied success at the Battle of Midway is a classic example of a victory made possible by cryptanalysis.

The dangers during peacetime stemming from the potential weakening of our cryptographic capabilities are less clear. The government does not admit the existence, much less success, of any of its specific cryptanalytic efforts, so it is more difficult to point to specific potential or actual damage

Best Available Copy

arising from the revelation of cryptographic information. There are other factors which encourage an intransigent skepticism about the real-world effects of wide-spread writing on cryptographic issues. The daily press carries more bone-chilling reports revealing American intelligence capabilities, with far wider circulation, than all of the learned academic and scientific publications combined. Some of our most carefully nurtured technological advances have suffered from a hemorrhage of foreign technology transfer, from international trade -- the licit or illicit selling of everything from chips to detailed manuals -- to explicit espionage efforts.

In addition, many members of the Public Cryptography Study Group expressed concern that a more expansive vision of the national interest should be recognized beyond what they saw as NSA's more narrow, military and foreign intelligence focus. In particular, they encouraged the Study Group to address the growing need for security for unclassified but sensitive personal, proprietary and financial communications and data. Some saw the possibility that any efforts to restrain publication of non-government research in cryptography would limit the nation's ability to use cryptography as an effective means of providing security.

Adding to the questions raised by some members of the Study Group was the fact that there was also some significant disagreement within the Government as to the need to control

Best Available Copy

97-341 0 - 82 - 17

dissemination of technical data. Some staff members of the Department of Commerce, in particular -- with an eye toward increased foreign commerce and international trade although with virtually no access to the classified, underlying intelligence data -- stated that there is only a minor impact on the national security from the wide-spread publication and export of technical data. The Departments of State and Defense, on the other hand, have continued to emphasize the need for effective control of the international transfer of technology.

Any resolution of this controversy must recognize this skepticism and the reasons for it, and must also take account of what is probably, in general, a healthy suspicion of the power of the Federal Government. Nonetheless, it is equally important to consider for a moment the views that NSA brought to this dialogue. NSA is an intelligence agency with extremely dedicated and capable personnel, who also happen to be very secretive. It has only been in the last dozen or so years that the Government has officially admitted that NSA exists and what its missions are. This reluctance to take a public posture is based in large part on a very realistic concern that the kind of intelligence gathering that NSA does is so tenuous and fragile -- so easily incapacitated by seemingly trival revelations -- that any public discussion of NSA's activities or the business of cryptography could irreparably damage its mission, thus seriously impairing the Government's ability to collect

Best Available Copy

intelligence or to make knowledgable and considered foreign policy decisions.

While this reticence is understandable, it has spawned other problems. In one incident, several years ago, an NSA employee--acting in his personal capacity--wrote a letter warning of the potential for violation of certain provisions of the national export control regulations in the presentations at an academic seminar of certain papers relating to cryptologic research. While NSA had no advance knowledge of the letter, the incident was generally interpreted, both in the media and by the academic community, as an attempt to stifle academic freedom. Some other actions during the same time frame involving patent secrecy had a similar effect. Looking back on these incidents that occurred in the mid-to-late 1970s, I think they suffered from an excess of zeal, but not from malicious intent. While NSA spokesmen were close-mouthed about the purposes for the official actions that occurred, this did not stem from an absence of rationale but from a genuine fear by NSA officials during that time that any extended public discussions of NSA's underlying concerns would harm intelligence efforts.

In this context, Vice-Admiral Inman's decision to "go public" on these issues was fairly remarkable. As the then Director of NSA, Adm. Inman expressed his concern that some information contained in published articles on cryptographic techniques endangered the successful accomplishment of NSA's

Best Available Copy

mission and, thus, the national security. He expressed the view that existing statutes do not regulate the domestic publication of unclassified information pertaining to cryptography and suggested that new legislation may be required. Initially, however, he proposed a dialogue with the academic community on how best to reconcile the national security needs as he saw them with the traditions of academic and scholarly freedoms.

As a starting point, Adm. Inman suggested that any restrictions or regulations that resulted should apply only to the central core of critical cryptographic information that is likely to have a discernible adverse impact on the national security. He suggested that any resulting statute or other restrictions should have criteria that are as narrow and specific as possible without revealing information damaging to the national security, and that the burden for imposing any restriction on dissemination should be with the government.

In response, a number of informal discussions and dialogues began. Ultimately, the American Council on Education ("ACE") proposed establishment of the Public Cryptography Study Group, which the National Science Foundation agreed to fund. In assembling the Study Group, ACE sought nominations from several professional societies and organizations. Six such organizations nominated persons, who served as individuals rather than representatives of their associations. The Study Group was co-chaired by Dean Baum of the College of Arts and

Best Available Copy

Sciences, the Florida State University, and Chancellor Heyman of the University of California at Berkeley, also a noted constitutional law scholar. The Study Group met publically a number of times from March 1980 until February 1981, and a number of observers were customarily present and were always permitted to participate fully in the Study Group's activities, except for the final voting.

The Study Group decided, after substantial and sometimes heated discussions, to accept as a working premise the proposition that some form of publication of some materials on cryptography could have an adverse impact on the national security. NSA's concerns were expressed as twofold: that articles in learned and professional journals may, first, potentially compromise U.S. code systems, and second, that they may reveal weaknesses in other governments' code systems, thereby eventually hindering U.S. efforts to collect intelligence.

It is impossible to prove the case that these concerns are real without revealing classified information. Accordingly, when skepticism about NSA's fears was originally raised by members of the Study Group, I suggested obtaining sufficient security clearances for all or some of the members of the Study Group so that the national security concerns could be set out in detail. The majority of the Group decided, instead, to accept the existence of a national security threat as a premise

Best Available Copy

from which to work. While this may not be entirely satisfactory, NSA was both willing and able to establish, at the proper clearance level, the scope of its concerns. In this light, I believe the charge that the Study Group's recommendations are faulty because NSA has failed to prove the basis of its concerns, to be disingenuous.

After careful consideration, and a number of very open and frank meetings, the Study Group decided to reject any statutory solution. That conclusion was based, in part, on some remaining unease about the Group's ability to assess the extent of the threat to national security -- even assuming its existence -- and difficulties in reaching a narrow and precise definition of what types of research would be covered by the proposal. There was also some strong feeling that a voluntary system is more likely to generate cooperation from affected researchers and authors than a compulsory system, such as might be expected from a legislative solution.

Instead, the Study Group recommended that a nonstatutory, voluntary program of pre-publication review be established by NSA in order to identify information that could be inimical to the national security if published. The Study Group stated that, in order for the system to be successful, NSA would have to convince authors of its necessity, wisdom and reasonableness by demonstrating sensitivity and a sense of restraint. The Study Group expressly stated that its recommendation was not to be construed as endorsing any legislation based on the proposed procedures.

Best Available Copy

With those caveats, the Study Group suggested the following guidelines to NSA for establishing the procedure:

(1) NSA should notify the interested community of its desire to review manuscripts concerning aspects of cryptology prior to publication, and should invite authors to send manuscripts to NSA for pre-publication review. The current Director of NSA, Gen. Lincoln Faurer, has taken that initiative and has indicated that NSA is establishing a formal pre-publication review procedure. In response, approximately 25 papers have been submitted for this review since mid-1981.

(2) NSA, in cooperation with appropriate technical societies and other interested persons, should define as precisely as possible those aspects of cryptology to be covered by the procedure. This step, NSA has discovered, has been particularly difficult. After one unsuccessful start, NSA indicated that, while only a limited amount of information may bear directly on NSA's missions, to describe such information in detail could be more damaging in terms of revealing U.S. capabilities than any benefit that might be derived from the information received from researchers. Additionally, NSA pointed out that the details of work already done or underway at NSA may become known through too detailed a description. Accordingly, NSA offered for comment a more general description of papers they would like to see. NSA stated:

> "We are especially interested in looking at papers that discuss or present the analysis and evaluation of cryptography (mechanical, manual, or computer-based systems, general or specific,

Best Available Copy

> whether intended for public or private use); specific cryptographic techniques or applications (for example, data encryption standard or techniques involving digital signature, authentication, etc.); and theoretical or actual evaluation methods (such as proofs of security or standards of cryptosystems)."

As seen from this proposed definition, NSA appears to be searching for a way to describe specific applications of cryptologic theory, without seeming to request all general mathematical or computer theory somehow remotely connected to cryptography.

The effort to reach agreement on a definition continues. I understand that NSA intends to pursue the question of the definition while making a general invitation to authors in the field of cryptography to submit materials for pre-publication review.

(3) It was also suggested that NSA should assure prompt review of submitted manuscripts and prompt response to authors with an explanation, to the extent feasible, of proposed changes. In this regard, NSA has committed to respond to all inquiries within 30 days, and most reviews of the 25 papers submitted so far have been handled within that period. No paper submitted so far has caused NSA any security concerns.

(4) Finally, the Study Group recommended that NSA establish an Advisory Committee of five persons, with full clearances, to make recommendations to the Director, NSA and to the author as to any matters in which there continued to be a disagreement between the author and the NSA staff. This

Best Available Copy

Advisory Committee was to provide its review promptly. NSA has established the Advisory Committee and has nominated two members to that committee. Under the Study Group proposal, the other three members of the Advisory Committee are to be recommended by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Science. I understand that this process is currently underway. The fact that the Advisory Committee is not yet in place, however, has not impaired the pre-publication review process because no papers so far submitted to NSA have raised security concerns and no controversies have had to be raised to the Advisory Committee.

Conclusion

This process, beginning with a dialogue between NSA and the academic community, was a fairly unique effort to bring together contesting interests to work together to seek to obtain a compromise that would recognize the interests of the different constituencies. So far, it has been fairly successful in that there has been a remarkably free sharing of views and concerns resulting, I believe, in a greater understanding on both sides of the others' interests. An in-depth appreciation of whether the pre-publication review system actually works will have to await more actual practice, probably to include some experience with how well the advisory committee meachanism will work.

Best Available Copy

Nonetheless, I believe we can make some observations. The Public Cryptography Study Group, and the dialogue that proceeded it and continues after it, represented an honest effort on the part of the government and the academic community to address a specific issue which involved questions of both national security and academic freedom. Although there are persons in both "camps" who are displeased with the result, it appears that an approach has evolved that includes the different constituencies working together to achieve a solution that should satisfy to a significant degree the needs and viewpoints of each.

In my view, the process worked here as well as it did for the following reasons:

- The issue, while involving greater interests, was defined sufficiently narrowly that it could be grasped reasonably easily. Efforts to enlarge the issues to ones of global significance would have made it impossible for the Study Group to comprehend or deal with the controversy.
- Most of the members of the Study Group were willing, over time, to appreciate -- although not always entirely accept -- the concerns of the others. This permitted sufficient common ground for the various members of the Study Group to be able to discuss rationally the issues.

Best Available Copy

- Despite some intense suspicion on both sides (and even some fairly recent, unfortunate disputes), members of both the national security and academic communities were willing to recognize that the other constituency existed and had its own legitmate and significant interests. Furthermore, members of each constituency recognized that members of the other constituencies were willing to enter discussions and make compromises, and recognized further that such efforts should be encouraged.
- The Study Group members were willing to consider the pre-publication review program on a trial basis. Further, NSA was willing to enter the experiment the success of which was dependent in part on the Agency's willingness and ability to act with restraint and sensitivity.
- ACE and NSF provided a non-threatening, neutral ground upon which the issues could be addressed.

Such a cooperative management of problems may well serve in the future as a model for handling similar issues that may be encountered by the government and the academic community.

Best Available Copy

The Progressive Case and the Need to Amend the Atomic Energy Act

A Paper Presented to

The American Association for the Advancement of Science

January 7, 1981

Congressman Paul N. McCloskey, Jr.

I wish to speak today on the "born secret" provisions of the Atomic Energy Act of 1954. The Government Information Subcommittee of the Committee on Government Operations has taken only a small first step on what will be a long and tortuous road towards solution of the serious uncertainty in the Act. During last year's hearings, the problems highlighted by The United States v. The Progressive, Inc., 467 F. Supp. 990 (W.D. Wis., 1979), were first considered on the Hill. This first step did no more than lay out the chronological order of events which led to our current problem. Congress owes a debt of gratitude to those who testified before the Subcommittee. But it owes an even greater obligation to the nation. As George Washington University law professor Mary Cheh pointed out nearly a year ago,

> "...given the unsatisfying conclusion of the Progressive litigation, it is imperative that Congress now confront the uncertainty it created when it first wrote a law with such sweeping yet ambiguous information control provisions." 1/

It is indeed imperative that Congress now act. Uncertainty in the law may be acceptable when the freedoms and reputations

---

1/ Mary M. Cheh, The George Washington Law Review, January 1980, p. 163, 210.

Best Available Copy

of ordinary citizens are not endangered, but for over two years now, the freedoms and reputations of ordinary citizens, and particularly honorable scientists have been endangered.

The problem lies in the "Born Secret" concept contained in the Atomic Energy Act of 1954, and has three elements: (1) the classification procedures and policies of the Department of Energy, (2) the ambiguity of the present law as it is being interpreted by the Energy and Justice Departments, and (3) increasing public dispersion of scientific data bearing on construction and use of weapons which can destroy mankind.

These factors have led to a situation whereby the Government is now depending on the threat of criminal prosecution to cow scientists, both government and private, into restraint in the communication of ideas, while conceding that if criminal prosecution were attempted, it would probably fail.

At stake is the ability of scientists, both inside and outside government, to communicate with each other and thus advance scientific knowledge. Balanced against this goal, which has historically been considered as a highly laudable one, looms our growing uneasiness, if not conviction, that controlled advancement of science in the fields of nuclear weaponry, biological welfare and perhaps other areas such as genetics can destroy the world.

Clearly, a balance is required between advancing science and protecting the public against a too-easy creation or

Best Available Copy

possession by terrorists of hydrogen bombs, nerve gas and laser weapons.

The balance struck in the 1954 Atomic Energy Act, however, is clearly no longer adequate.

The question now is whether Congress will have the perserverance to continue to search for a solution, or, in the alternative that the current Administration will care enough to participate in such search.

The situation created by the Progressive decision, handed down March 26, 1979, is this:

Whenever an individual, public employee or private citizen, generates a new concept of nuclear weaponry, that concept is "Born Secret" and, under the law, becomes classified information upon creation due to the statutory definition of Restricted Data.

But only the government can classify.

And, only the government can declassify. But declassification is easily accomplished. It occurs when the Government permits one of its scientists to do so. It can occur merely by putting information on the shelves of a public library.

The relevant section of the Atomic Energy Act Section 2014(11) (6) defines restricted data . . . that which is prohibited from publication . . . as:

> "all data concerning (1) design, manufacture, or utilization of atomic weapons: (2) the production of specific nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 2162 of this title." (emphasis added)

Best Available Copy

The last phrase is crucial. Restricted data does not include data which the government has declassified, i.e., allowed to be published in the public domain.

A great deal has been published in the public domain in recent years, most of it by distinguished government scientists like Edward Teller, Ted Taylor and George Rathjens.

From that mass of published information, and following questioning of several government scientists, an astute but scientifically unlettered newspaper reporter, Howard Morland, prepared an article for publication in The Progressive Magazine. Morland contends that he had described nothing more than information which had lawfully been "removed from the 'Restricted Data' category" through information released into the public domain. The Court felt otherwise, finding that the article contained "concepts" not previously published.

The Court's language focuses on a hard reality:

> "Faced with a stark choice between upholding the right to continued life and the right to freedom of the press, most jurists would have no difficulty in opting for the chance to continue to breathe and function as they work to achieve perfect freedom of expression."

In effect, the court found that the threat of life represented by unrestricted publication of H-bomb facts justified prior restrain of that publication.

During the court proceedings, a private citizen who was also an amateur nuclear weapons enthusiast reached the conclusion that the Department of Energy was managing its classification program improperly. This private citizen, Charles Hansen,

Best Available Copy

contended that DOE had permitted leading government scientists in years past to publish the basic concepts of nuclear weaponry, but was now applying a different standard to private citizens such as Howard Morland.

Hansen felt that any "concepts" presented by Morland were easily deducible from already-published data.

Hansen had sent an 18-page letter to three Members of Congress and several newspapers containing his views. When the government learned of the letter, the Department of Energy classified it and the Justice Department sought to prohibit the Daily Californian from publishing it. However, the Madison Press Connection, on September 16, 1979, published Hansen's letter in its entirety, rendering moot the Progressive controversy, and causing the Justice Department to drop its lawsuit.

Hansen had done nothing more than any private citizen might have done in reading public journals and studying data available to the public.

At least seven other people during the past several years have sent communications relating to nuclear weaponry concepts which they believed, in good faith, to contain information which had been properly declassified, only to have it promptly classified by the Department of Energy.

For example, in May of 1978, Dmitri Rotow, a Harvard student, found in the Los Alamos Public Library a document called "Final Design Status of the TX-7" and proceeded to write a paper on its content. Subsequently, his paper was classified by the

Best Available Copy

Department of Energy. A year later, Rotow returned to the Library to research the public availability of information on nuclear weapons for the American Civil Liberties Union. He then discovered document number UCRL 4725 and made copies of it. A librarian, observing his work, discovered that the document had been wrongly declassified.

Drs. Postol, Marsh, Stanford and DeVolpi at the Argonne National Laboratory have also maintained that the Department of Energy is manipulating the classification procedures for political purposes.

On April 25, 1979, during the Progressive case, they wrote a letter to Senator John Glenn concerning alleged misuse of the Department of Energy's classification procedures. The Department of Energy then classified their letter. Significantly, The Department of Energy did not remove such classification until one day before the Government Operations Subcommittee held public hearings on the question in March, 1980.

Two scientists at the Lawrence Livermore National Laboratory, Dr. Hugh DeWitt and Dr. Ray Kidder, sent a memo to the regents of the University of California concerning the declassification of the Inertial Confinement Fusion Program. The Department of Energy immediately classified their memo.

Note that nine reputable individuals, six government employees and three private citizens, have therefore been able to generate communications in good faith, believing them to contain already-

Best Available Copy

published information which the government subsequently chose to classify.

The six government employees all believed that the Department of Energy had used its classification procedures for political purposes rather than in checking bona fide breaches in order to protec nuclear secrecy.

What was the result? For months the Energy Department and the Justice Department hinted darkly at possible criminal prosecution of the scientists. Finally, on September 4, 1980, the Justice Department conceded that it would not prosecute.

The ranking Republican Member of the House Armed Services Committee had previously criticized Justice for not enforcing the law. Congressman Wilson wrote, on January 31, 1980:

> "Notwithstanding the adequacy of existing laws, to prevent or deter the spread of Restricted Data, there has been a reluctance by the FBI and the Department of Justice to aggressively investigate and prosecute alleged violations. Without enforcement, no amendment to the law should make any difference."

Congressman Wilson's view was shared by top Department of Energy officials who claimed that the FBI and Department of Justice have been remiss in meeting their responsibilities under the 1954 act. The Department of Energy apparently

Best Available Copy

felt that Morland, Hansen and Rotow, at least, could not have derived their new concepts had not someone at the Department "leaked" information. Both the Department of Justice and the FBI, at the congressional hearings in March 1980, indicated that they held little hope of successfully prosecuting private citizens under the 1954 Act, since to be guilty of any offense the private citizen would have to be proven guilty beyond a reasonable doubt, in the unanimous view of twelve fellow citizens that he published his ideas "with intent to injure the United States,... or with reason to believe such data will be utilized to injure the United States." (42 U.S.C. § 2274). Most prosecutors and defense attorneys would agree completely. The chilling effect on government scientists is far more deadly, however. A government scientist can be prosecuted if he "knowingly communicates, or conspires to communicate or to receive, any restricted data, to any person not authorized to receive Restricted Data, or having reason to believe that such data is Restricted Data, to any person not authorized to receive Restricted Data... upon conviction thereof, be punishable by a fine not more than $2,500." 42 U.S.C. § 2277. (emphasis added)

At the Subcommittee's hearings on March 20, 1980, the Department of Energy argued that the law might have been violated and that the threat of prosecution was part of their policy. In response to a suggestion that it was the threat

Best Available Copy

of the use of the law rather than the law itself which was the key weapon in the Department of Energy's armory; Mr. Fygi, Deputy General Counsel for DOE, answered:

"That may be very well true in this case as in other cases."

When it was then suggested that by delaying the eforcement of the law and holding the threat availiable, the Department of Energy was trying to chill the scientists from further communication: Mr. Fygi replied:

"It may describe a result or consequence, but not any deliberate policy".

It was not until September 4, 1980, nearly a year and a half after the Progressive decision, that the Energy Department and the Justice Department finally conceded that neither the scientists nor the private citizens involved in the Progressive case would be prosecuted.

Under these conditions, we have the unusual circumstances of the Department of Energy threatening its own scientists with the black cloud of dishonor and criminal prosecution, not because the law is clear, but because it is unclear!

Best Available Copy

This is, in effect, a rule of men, not of law. Respect for the law has never been more necessary, but that respect traditionally has been based on the premise that the law is clear and unambiguous and everyone is presumed to understand it. The law should not be a tool available to an embarrassed bureaucrat to threaten an honorable employee in order to cover his own political hindquarters.

As Professor Cheh said, it is imperative that Congress now act.

The Energy and Justice Departments' positions under the Carter Administration were dangerous in that they could encourage our best scientists of the future to remain in private life rather than serve the government and risk irreparable damage to their reputations.

Likewise, if a Harvard student, a newspaper reporter and an untrained nuclear amateur can generate articles gathered from publicly-available sources, which the government feels must be kept secret because those articles threaten the peace of the world, the law is clearly no longer adequate to protect the national security.

What can the Reagan Administration do? After months of consideration, Deputy Attorney General Ed Schmultz has written that the Justice Department no longer uses the threat of prosecution to inhibit scientific exchange. The new Secretary of Energy has apparently not yet addressed the problem.

Best Available Copy

This, of course, returns the burden to Congress. It would now seem appropriate for the committees of jurisdiction to invite the leading members of the U.S. scientific community (and their lawyers) to come forward with specific recommendations. A new law is needed which will set out a new balance between the need for free communication of scientific concepts and the need to protect against every American being able to add a nuclear weapon to his handgun collection. What that balance should be is apparently beyond the comprehension, will, or desire of the lawyers of the Departments of Energy and Justice. It can only be resolved by Congress.

In order to focus the debate, I introduced a bill based on a conceptual design proposed by Dr. DeVolpi. It is designed to do two things:

(1) change the definition of "Restricted Data" to omit lawfully published data or that which is derived from such data, thus allowing private citizens to act without fear of prosecution when they lawfully publish articles, magazines, papers, or other reports.

(2) require that if private citizens are to be punished for violation of the Act, that they have a specific intent to injure the United States or help a foreign nation, and are not subject to prosecution merely because the Department of Energy thinks they should have "reason to believe" they will harm the U.S. or help a foreign nation.

97-341 0 97

Best Available Copy

This bill has yet to achieve any legislative action or even attention. Referred to the Committee on Interior and Insular Affairs, the committee of jurisdiction over energy, the Committee declined jurisdiction. The Committee on Government Operations is uninterested in holding further hearings. While sparking some interest in the House Armed Services Committee, no hearings have yet been held or scheduled in the 97th Congress, the Armed Services Committee being unwilling to move until the Administration takes a position. The impasse rivals Catch 22.

Professor Cheh's admonition remains sound. Congress should act.

As 1982 begins, perhaps the considered and unanimous agreement of this Association could be the lever necessary to force the Administration to take a position. The weight of judgment of distinguished private citizens, accompanied, in due course, by appropriate media interest, has been known to force even the busiest of bureaucrats and politicians to give attention to an outraged public's concerns.

Respectfully Submitted,

PAUL N. McCLOSKEY, JR.

Best Available Copy

LETTERS FROM THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA TO THE U.S. TRADE REPRESENTATIVE

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

RICHARD L. LESHER
PRESIDENT

1615 H STREET, N.W.
WASHINGTON, D.C. 20062
202/659-6207

March 1, 1982

The Honorable William E. Brock
U.S. Trade Representative
Winder Building
600 17th Street, N.W.
Washington, D.C. 20506

Dear Bill:

I wrote you in April of last year to express the Chamber's views regarding the use of trade sanctions. I would again like to reiterate the U.S. business community's support for legitimate national security and foreign policy export controls and applaud the Administration for its efforts to achieve a multilateral consensus within the Western Alliance on the use of these controls. However, we continue to be concerned over unilateral export controls imposed for foreign policy purposes when those controls succeed only in penalizing the U.S. exporter. If it could be demonstrated that such controls achieve the stated objective either of harming our adversaries or in forcing a change in their behavior, I believe U.S. business would be prepared to support the Administration and forgo export sales to these countries. However, if these foreign policy controls result merely in a loss of sales to our trade competitors without any significant effect on our adversaries, we must question the appropriateness of such controls.

In this regard, I would again like to commend the Administration for its decision last year to lift the Soviet grain embargo. As Secretary of Agriculture Block recently stated, U.S. agricultural embargoes have had the short-term effect of depressing farm prices and the longer-term impact of closing off markets and stimulating foreign competition. Agricultural embargoes also have proven to be costly to American taxpayers and detrimental to this country's economic growth and efficiency. As Secretary Block documented before the Senate Agricultural Committee, the existence of alternate suppliers has caused U.S. agricultural embargoes to be both ineffective in harming our adversaries or in forcing a change in their behavior.

Best Available Copy

We are in full agreement with the Secretary's views, but believe that the applicability of his findings goes far beyond the agricultural field. The trade-diverting effects of sanctions have been well documented by a number of companies which have seen export sales of their commodities, equipment or technology embargoed in recent years. Several other American companies, the export sales of which have reportedly been considered for sanction, have information indicating that such potential sanctions would likely result only in lost U.S. exports rather than any significant foreign policy gains. Should you wish information in this regard, we would be most pleased to put you in contact with these companies.

I bring this to your attention in light of the Administration's current review of its sanction policy. As was the case with the agricultural embargo, we urge the Administration to weigh carefully the short and long-term economic consequences of any present sanctions. We also urge the Administration to examine carefully the probable domestic economic impact, as well as likely effectiveness of any additional sanctions, prior to any future decisions in this area.

I would like to conclude by again emphasizing that U.S. business is prepared to support the actions of this Administration and to forgo export sales, if by doing so we contribute to the national interest of the United States. However, if such actions result merely in the loss of sales to our trade competitors without significantly impacting upon our adversaries, then we must question whether we are sacrificing our export goals for no apparent national gains.

Sincerely,

Richard L. Lesher

cc: The Honorable Malcolm Baldrige
The Honorable Alexander Haig
The Honorable Edwin Meese III
The Honorable William Clark

Best Available Copy

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

April 23, 1981

RICHARD L. LESHER
PRESIDENT

1615 H STREET, N.W.
WASHINGTON, D.C. 20062
202/659-6207

The Honorable William E. Brock
U.S. Trade Representative
Winder Building
600 17th Street, N.W.
Washington, D.C. 20506

Dear Bill:

I am writing to you in your capacity as chairman of the Trade Policy Committee. It is our hope that the Committee will work closely with the U.S. business community for the establishment of a coherent U.S. trade policy. In particular, we hope that business views will be factored into the formation of an export administration policy.

The Export Administration Act of 1979 recognizes that uncertainties in export control policy may curtail the efforts of American business to the detriment of the U.S. balance of trade. The U.S. Chamber was an early and vocal supporter of the Act in the belief that the legislation created an equitable balance between legitimate security and policy concerns and the need to increase American exports. However, the proliferation of new export controls on the grounds of foreign policy and national security has contributed to further uncertainty and frustration on the part of U.S. exporters.

American policymakers have viewed export sanctions erroneously as an effective and relatively inexpensive means by which to achieve the country's political objectives. This view is an outgrowth of the days when the United States was the preeminent economic power of the world and in many instances the sole international supplier of equipment and technology. Although this no longer is the case, policymakers in this country have exhibited an increasing tendency to use trade as a means to further such goals as the suppression of international terrorism, the enhancement of human rights, or the cessation of military aggression.

Best Available Copy

Trade sanctions have not had a clear record of success whether imposed multilaterally (Southern Rhodesia) or unilaterally (South Africa). The most dramatic use in recent years of U.S. trade sanctions were those imposed in response to the Soviet invasion of Afghanistan. In light of the current review of U.S.-Soviet relations, we believe this is an appropriate time for the new Administration to examine these and other sanctions to determine whether they have had their intended effect and to measure this effect against the costs of such sanctions to the United States. In this regard, the experiences of some of our member companies may be of interest.

As you know, several U.S. firms trace their commercial ties with the Soviet Union back to the 1920s. However, with the direct support and encouragement from the U.S. Government in the 1970s, many other businesses began to develop Soviet trade ties for the first time. We know that a number of these companies are reevaluating their commercial relationships with the USSR. It is clear now that, unless a degree of predictability is returned to the U.S. commercial decision-making process and a considerable measure of trade is restored, many companies will cease doing business in the Soviet market altogether.

Perhaps the best single example during the past year of the apparent ineffectiveness of trade sanctions involves Soviet efforts to construct a steel mill for the production of electrical steel at Novolipetsk. American companies had negotiated for as long as five years to participate in this project, and of the $353 million to be invested in the project, it was expected that $100 million in orders for U.S. equipment would result. With the imposition of U.S. sanctions, the U.S. contracts were terminated and awarded shortly thereafter to the French.

Another major project involved negotiations for the construction of an aluminum smelting complex at Sayansk. In this instance, an American company was forced to pull out of the final stage of negotiations, which would have likely resulted in the purchase of another $100 million in American equipment and technology. In this case, the West Germans were the recipients of the business lost by the United States.

Another major deal which might have resulted in American sales of some $100 million involved Soviet purchases of equipment for a project in that country's energy infrastructure. In this case, American suppliers traditionally serving Soviet needs in this area were not even invited to bid on the equipment. Instead, the Soviet Union turned to the Japanese for the necessary equipment.

Best Available Copy

Loss of participation in these three projects alone has meant a loss of some 5-6,000 potential jobs in this country, based on U.S. Department of Commerce multipliers. If this loss were measured against benefits to our national security, such as an inability of the Soviets to proceed with these projects, U.S. business would be less critical of the actions of our government. As it is, the projects are going ahead and the potential U.S. jobs have been merely given up to our trade competitors.

With the embargo on phosphate sales to the Soviet Union, again U.S. sanctions have had little effect other than to harm U.S. commercial interests. Since the embargo, the Soviets have obtained alternate supplies of phosphates from Tunisia, Morocco, Belgium and South Africa. Even more disturbing and far reaching is the fact that the Soviets have begun discussions with France and Morocco concerning the possible construction of superphosphoric acid plants to satisfy long-term Soviet needs. U.S. sanctions, rather than harming the Soviets, have put the United States in the position where it stands to lose tens of millions of dollars worth of sales to the Soviet Union and have encouraged the creation of a permanent competition for U.S. suppliers.

Because of U.S. price supports and government purchase programs, it is much more difficult to assess the direct economic impact on U.S. agriculture of the U.S. embargo to the Soviets of grain and other agricultural commodities. Perhaps a more important question is the long-term effects on future trading patterns resulting from a Soviet perception of commercial unreliability of U.S. agricultural suppliers. The economic impact on the Soviet Union of the grain embargo is also open to question. According to original Department of Agriculture projections, the cancellation of 17 million metric tons of U.S. grain shipments would result in a total Soviet shortfall of 8-13 million metric tons. Some recent estimates, however, place Soviet grain imports last year as high as 36 million metric tons, which, if true, would seriously call into question the effectiveness of the U.S. embargo.

There are numerous other examples where opportunities for U.S. sales were sacrificed to the advantage of our trade competitors without any perceivable impact on the Soviet economy. This is particularly true in the electronics and energy fields. In addition, such losses have a multiplier effect on related fields, such as transportation and insurance.

In light of these results, the U.S. Chamber offers the following recommendations for consideration by the Trade Policy Committee:

Best Available Copy

First, the President's ability to employ export controls to further our national security should be continued. Such controls, if undertaken within the letter and spirit of U.S. law, should be supported. Implicitly, however, this requires real determination of the actual contribution of U.S. exports to the military potential of an adversary country. Furthermore, the imposition of such controls, except under the most extreme circumstances, should be multilateral in nature, with the full support of our allies.

Second, there is ample evidence that the unilateral imposition of trade sanctions has been ineffective in changing foreign behavior. Recent sanctions invoked for foreign policy purposes have been imposed without due regard to the provisions of the Export Administration Act requiring the President to determine the likelihood that export controls will attain foreign policy objectives and determine the probable domestic economic consequences of such sanctions. The existence of alternate suppliers of goods, technologies and services has undermined the effectiveness of unilaterally imposed export controls, and as a result, these controls have had merely a symbolic rather than substantive effect. Consequently, we believe that unilateral trade sanctions for foreign policy purposes should be avoided as they have proven to be costly in terms of lost exports, foregone markets, and allegations of commercial unreliability.

If the President determines that the employment of economic tools to achieve foreign policy goals is essential, consideration should be given to broadening the sanctions to include all facets of economic interaction, including investments, imports, and services such as transportation, insurance and banking. There is no reason why the U.S. export sector alone should be forced to shoulder the burden of U.S. policy decisions. Furthermore, we believe that the President, when faced with the possibility of restraining all facets of trade and economic cooperation, may give closer consideration to the economic consequences of foreign policy sanctions and, therefore, invoke such controls in only the most serious situations.

We hope these recommendations will be of value in the course of your reevaluation of U.S. trade policy. We believe there is an urgent need to return a degree of consistency and predictability to the U.S. export administration process and view this as a key step in any program to improve the competitiveness of U.S. exports abroad.

Sincerely,

Richard L. Lesher

cc: The Honorable Malcolm Baldrige, Secretary of Commerce
The Honorable Alexander Haig, Secretary of State
The Honorable Edwin Meese III, Counsellor to the President

Best Available Copy